

PCT

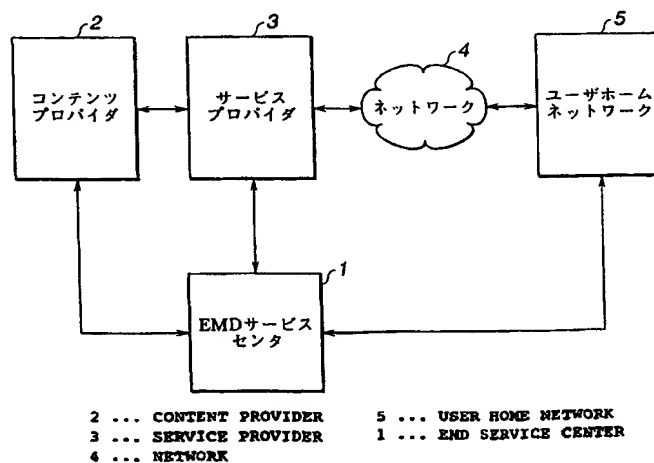
世界知的所有権機関  
国際事務局

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7 <b>G06F 15/00, 17/60, H04L 9/08</b>	<b>A1</b>	(11) 国際公開番号 <b>WO00/22539</b>  (43) 国際公開日 2000年4月20日 (20.04.00)
(21) 国際出願番号 PCT/JP99/05689  (22) 国際出願日 1999年10月14日 (14.10.99)  (30) 優先権データ 特願平10/293830 1998年10月15日 (15.10.98) JP 特願平10/296942 1998年10月19日 (19.10.98) JP 特願平10/313020 1998年11月4日 (04.11.98) JP 特願平11/103337 1999年4月9日 (09.04.99) JP  (71) 出願人 (米国を除くすべての指定国について) ソニー株式会社 (SONY CORPORATION) [JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)		(72) 発明者; および (75) 発明者/出願人 (米国についてののみ) 松山科子 (MATSUYAMA, Shinako) [JP/JP] 石橋義人 (ISHIBASHI, Yoshihito) [JP/JP] 北原 淳 (KITAHARA, Jun) [JP/JP] 浅野智之 (ASANO, Tomoyuki) [JP/JP] 北村 出 (KITAMURA, Izuru) [JP/JP] 大澤義知 (OSAWA, Yoshitomo) [JP/JP] 大石丈於 (OISHI, Tateo) [JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo, (JP)  (74) 代理人 小池 晃, 外 (KOIKE, Akira et al.) 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo, (JP)  (81) 指定国 AU, CA, CN, KR, SG, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)  添付公開書類 国際調査報告書 請求の範囲の補正の期限前の公開; 補正書受領の際には再公開される。

(54) Title: INFORMATION PROVIDING SYSTEM

(54) 発明の名称 情報提供システム



## (57) Abstract

A content provider (1) adds a dealing policy to a ciphered content and transmits the content with the dealing policy to a service provider (3). The service provider (3) calculates and adds to them the charge from the dealing policy and transmits them to a user home network (5). The user home network (5) creates charging information according to the use of the content, and transmits the information with the dealing policy to an EMD service center (1). The EMD service center (1) detects fraudulence from the charging information, dealing policy, and the charge.

(57)要約

課金処理モジュール 7 2 は、情報の使用の許諾条件を示す情報を生成し、復号/暗号化モジュール 7 4 は、許諾条件を示す情報の認証情報を生成し、記憶モジュール 7 3 は、認証情報を記憶する。

PCTに基づいて公開される国際出願のパフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AL	アルバニア	EE	エストニア	LC	セントルシア	SD	スーダン
AM	アルメニア	ES	スペイン	LI	リヒテンシュタイン	SE	スウェーデン
AT	オーストリア	FI	フィンランド	LK	スリランカ	SG	シンガポール
AU	オーストラリア	FR	フランス	LR	リベリア	SI	スロベニア
AZ	アゼルバイジャン	GA	ガボン	LS	レソト	SK	スロヴァキア
BA	ボスニア・ヘルツェゴビナ	GB	英国	LT	リトアニア	SL	シエラ・レオネ
BB	バルバドス	GD	グレナダ	LU	ルクセンブルグ	SN	セネガル
BE	ベルギー	GE	グルジア	LV	ラトヴィア	SZ	スワジランド
BF	ブルキナ・ファソ	GH	ガーナ	MA	モロッコ	TG	トーゴ
BG	ブルガリア	GM	ガンビア	MC	モナコ	TD	チャド
BJ	ベナン	GN	ギニア	MD	モルドヴァ	TG	タンザニア
BR	ブラジル	GW	ギニア・ビサウ	MG	マダガスカル	TZ	タンザニア
BY	ベラルーシ	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア共和国	TM	トルクメニスタン
CA	カナダ	HR	クロアチア	ML	マリ	TR	トルコ
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	TT	トリニダード・トバゴ
CG	コンゴ	ID	インドネシア	MR	モーリタニア	UA	ウクライナ
CH	スイス	IE	アイルランド	MW	マラウイ	UG	ウガンダ
CI	コートジボアール	IL	イスラエル	MX	メキシコ	US	米国
CM	カメルーン	IN	インド	NE	ニジェール	UZ	ウズベキスタン
CN	中国	IS	アイスランド	NL	オランダ	VE	ヴェネズエラ
CR	コスタ・リカ	IT	イタリア	NO	ノルウェー	VG	ヴァイエトナム
CY	キプロス	JP	日本	NZ	ニュージーランド	YU	ユーゴスラビア
CZ	チェッコ	KE	ケニア	PL	ポーランド	ZA	南アフリカ共和国
DE	ドイツ	KG	キルギスタン	PT	ポルトガル	ZW	ジンバブエ
DK	デンマーク	KP	北朝鮮	RO	ルーマニア		
		KR	韓国				

## 明細書

## 情報提供システム

## 技術分野

本発明は、暗号化された情報を提供する情報提供システム、情報処理装置及び方法、管理装置及び方法、情報利用システム、プログラム提供媒体、情報記憶媒体並びに外部記憶媒体に関する。

## 背景技術

音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、再生する情報提供システムがある。

このような情報提供システムでは、暗号化された情報を復号するのに必要な鍵は、盗聴などの攻撃から情報を保護するため、所定のタイミングで変更される。また、上記情報提供システムにおいて、送信される情報は、署名が付されることにより、送信の途中で改竄された場合に、改竄されたことを検出できる。また、上記情報提供システムにおいて、ユーザは、複数の情報処理装置で情報を受信し、利用することができる。情報提供者は、複数の情報提供者に情報を送信し、サービスを提供することができる。上記情報処理装置にお

いて、情報の復号に必要な鍵及び課金情報など所定の情報は、外部からの不正アクセスを排除できる記憶部に記憶される。

しかしながら、定期的に鍵を配送するシステムにおいては、鍵の変更のタイミングと鍵の配送のタイミングがずれ、ユーザがデータを復号できないことがある。

また、送信される情報に署名が付されていても、正当な鍵を有する者の不正は、署名では検出できない。

また、ユーザは、契約のために、所定の手続をせねばならず、情報の提供者は、契約を要求するユーザの契約の可否を調査しなければならず、手間がかかり、契約成立までに時間がかかる課題があった。また、情報の提供者は、契約したユーザが不正を行った場合、それを発見するのが困難であった。

また、複数の情報処理装置を有するユーザは、それぞれの情報処理装置毎に、契約し、利用料金を精算しなければならず、手間がかかる。

また、利用内容を示す情報を書き換えることにより、所定の料金を支払わずに、例えば、再生の回数の制限を解除する、又は、再生のみからコピーも可能とするなど、利用内容を変更することができてしまう。

また、情報提供者は、複数のユーザ毎に、契約し、利用料金を精算しなければならず、また、精算処理及び利益の算出処理を行わなければならず、無駄が多い。

さらに、新たな機器を利用する場合、情報の提供者と再度、契約を行う必要がある。また、何らかの原因で、外部からの不正アクセスを排除できる記憶部に記憶された情報が破壊された場合、ユーザ



には、契約しているにもかかわらず、情報が利用できず、情報提供者には、利用済みの情報に対する課金情報等が利用できなければ、決済が不可能になるなどの問題が発生する。また、外部からの不正アクセスを排除できる記憶部に記憶される情報をそのまま外部に記憶したのでは、不正に対する安全性が低下する。

#### 発明の開示

そこで、本発明は、このような状況に鑑みてなされたものであり、データ提供側が任意のタイミングで鍵を変更したとしても、ユーザが、常に、暗号化された情報を、確実に復号することができるようにすることを目的とする。

また、本発明の他の目的は、情報の復号のとき、情報を暗号化する鍵が読み出されないようにすることにある。

また、本発明の他の目的は、正当な鍵を有する者の不正を検出できるようにすることにある。

また、本発明の他の目的は、ユーザが簡単に情報提供の契約ができ、提供者も迅速にユーザの契約の可否が判断できることできるとともに、契約したユーザの不正行為や授受される情報の正当性を容易に確認することができるようにすることにある。

また、本発明の他の目的は、利用内容を示す情報の書換えを検知し、対応できるようにすることにある。

また、本発明の他の目的は、精算処理及び利益の算出の処理を効率的にできるようにすることにある。

さらに、本発明の他の目的は、不正に対する安全性を保持したま

ま、必要な情報を外部に記憶できるようにすることにある。

本発明では、暗号化された情報、前記情報を復号する暗号化された第１の鍵及び前記第１の鍵を復号する第２の鍵を受信し、前記情報を復号するに当たり、第１の鍵を第２の鍵で復号し、復号できなかったとき、第２の鍵の送信を要求する。

すなわち、本発明は、暗号化された情報、前記情報を復号する暗号化された第１の鍵及び前記第１の鍵を復号する第２の鍵を受信し、前記情報を復号する情報処理装置において、第１の鍵を第２の鍵で復号する復号手段と、復号手段が第１の鍵を復号できなかったとき、第２の鍵の送信を要求する要求手段とを備えることを特徴とする。

また、本発明は、暗号化された情報、前記情報を復号する暗号化された第１の鍵及び前記第１の鍵を復号する第２の鍵を受信し、前記情報を復号する情報処理方法において、第１の鍵を第２の鍵で復号する復号ステップと、復号ステップで第１の鍵を復号できなかったとき、第２の鍵の送信を要求する要求ステップとを含むことを特徴とする。

さらに、本発明に係るプログラム提供媒体は、暗号化された情報、前記情報を復号する暗号化された第１の鍵及び前記第１の鍵を復号する第２の鍵を受信し、前記情報を復号する情報処理装置に、前記第１の鍵を前記第２の鍵で復号する復号ステップと、前記復号ステップで前記第１の鍵を復号できなかったとき、前記第２の鍵の送信を要求する要求ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明では、暗号化された情報、前記情報を復号する暗号化された第１の鍵及び前記第１の鍵を復号する第２の鍵を受信し、

前記情報を復号するに当たり、課金の値が所定の値に達したとき、第 2 の鍵の送信を要求する。

すなわち、本発明は、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を受信し、前記情報を復号する情報処理装置において、課金のための処理を実行する課金手段と、前記課金手段による課金の値が所定の値に達したとき、前記第 2 の鍵の送信を要求する要求手段とを備えることを特徴とする。

また、本発明は、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を受信し、前記情報を復号する情報処理方法において、課金のための処理を実行する課金ステップと、前記課金ステップでの課金の値が所定の値に達したとき、前記第 2 の鍵の送信を要求する要求ステップとを含むことを特徴とする。

さらに、本発明に係る情報提供媒体は、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を受信し、前記情報を復号する情報処理装置に、課金のための処理を実行する課金ステップと、前記課金ステップでの課金の値が所定の値に達したとき、前記第 2 の鍵の送信を要求する要求ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

本発明では、所定の管理装置が管理するシステムから、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を受信し、前記情報を復号するに当たり、情報処理装置を特定するデータを記憶し、情報処理装置を特定する

データを管理装置に送信し、情報処理装置を特定するデータを送信するとき、第 2 の鍵の送信を要求する。

すなわち、本発明は、所定の管理装置が管理するシステムから、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を受信し、前記情報を復号する情報処理装置において、前記情報処理装置を特定するデータを記憶する記憶手段と、前記情報処理装置を特定するデータを前記管理装置に送信する送信手段と、前記情報処理装置を特定するデータを送信するとき、前記第 2 の鍵の送信を要求する要求手段とを備えることを特徴とする。

また、本発明は、所定の管理装置が管理するシステムから、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を受信し、前記情報を復号する情報処理方法において、前記情報処理装置を特定するデータを記憶する記憶ステップと、前記情報処理装置を特定するデータを前記管理装置に送信する送信ステップと、前記情報処理装置を特定するデータを送信するとき、前記第 2 の鍵の送信を要求する要求ステップとを含むことを特徴とする。

さらに、本発明に係るプログラム提供媒体は、所定の管理装置が管理するシステムから、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を受信し、前記情報を復号する情報処理装置に、前記情報処理装置を特定するデータを記憶する記憶ステップと、前記情報処理装置を特定するデータを前記管理装置に送信する送信ステップと、前記情報処理装置を特定するデータを送信するとき、前記第 2 の鍵の送信を要求する

要求ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

本発明では、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を使用し、前記情報を復号する、第 1 の記憶手段及び第 1 の復号手段を有する情報処理装置において、相互認証し、一時鍵を生成し、第 2 の鍵を記憶し、第 2 の鍵で第 1 の鍵を復号し、第 1 の鍵を一時鍵で暗号化し、一時鍵で第 1 の鍵を復号し、第 1 の鍵で情報を復号する。

すなわち、本発明は、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を使用し、前記情報を復号する、第 1 の記憶手段及び第 1 の復号手段を有する情報処理装置において、前記第 1 の記憶手段は、前記第 1 の復号手段と相互認証し、一時鍵を生成する第 1 の相互認証手段と、前記第 2 の鍵を記憶する第 2 の記憶手段と、前記第 2 の鍵で前記第 1 の鍵を復号する第 2 の復号手段と、前記第 1 の鍵を前記一時鍵で暗号化する暗号化手段とを備え、前記第 1 の復号手段は、前記第 1 の記憶手段と相互認証し、一時鍵を生成する第 2 の相互認証手段と、前記一時鍵で前記第 1 の鍵を復号する第 3 の復号手段と、前記第 1 の鍵で前記情報を復号する第 4 の復号手段とを備えることを特徴とする。

また、本発明は、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を使用し、前記情報を復号する記憶手段及び復号手段を有する情報処理装置の情報処理方法において、前記記憶手段は、前記復号手段と相互認証し、一時鍵を生成する第 1 の相互認証ステップと、前記第 2 の鍵を記憶する記憶ステップと、前記第 2 の鍵で前記第 1 の鍵を復号する第 1

の復号ステップと、前記第 1 の鍵を前記一時鍵で暗号化する暗号化ステップとを含み、前記復号手段は、前記記憶手段と相互認証し、一時鍵を生成する第 2 の相互認証ステップと、前記一時鍵で前記第 1 の鍵を復号する第 2 の復号ステップと、前記第 1 の鍵で前記情報を復号する第 3 の復号ステップとを含むことを特徴とする。

さらに、本発明に係るプログラム提供媒体は、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を使用し、前記情報を復号する記憶手段及び復号手段を有する情報処理装置の、前記記憶手段に、前記復号手段と相互認証し、一時鍵を生成する第 1 の相互認証ステップと、前記第 2 の鍵を記憶する記憶ステップと、前記第 2 の鍵で前記第 1 の鍵を復号する第 1 の復号ステップと、前記第 1 の鍵を前記一時鍵で暗号化する暗号化ステップとを含む処理を実行させ、前記復号手段に、前記記憶手段と相互認証し、一時鍵を生成する第 2 の相互認証ステップと、前記一時鍵で前記第 1 の鍵を復号する第 2 の復号ステップと、前記第 1 の鍵で前記情報を復号する第 3 の復号ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

本発明では、暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムにおいて、暗号化された情報に、情報の取扱いを示す情報を付加して、送信し、送信された情報の取扱いを示す情報を基に、情報の使用料を算出し、暗号化された情報に、使用料を付加して、送信

し、使用料を基に、情報の利用に応じた課金情報を作成し、課金情報を、情報の取扱いを示す情報及び使用料の一部又は全部とともに、送信し、課金情報、情報の取扱いを示す情報及び使用料の一部又は全部から不正を検出する。

すなわち、本発明は、暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムにおいて、前記情報提供装置は、前記暗号化された情報に、情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第1の送信手段を備え、前記情報配布装置は、前記情報提供装置から送信された情報の取扱いを示す情報を基に、前記情報の使用料を算出する算出手段と、前記暗号化された情報に前記使用料を付加して、前記情報処理装置に送信する第2の送信手段とを備え、前記情報処理装置は、前記使用料を基に前記情報の利用に応じた課金情報を作成する課金情報作成手段と、前記課金情報を、情報の取扱いを示す情報及び使用料の一部又は全部とともに、前記管理装置に送信する第3の送信手段とを備え、前記管理装置は、前記課金情報、情報の取扱いを示す情報及び使用料の一部又は全部から不正を検出する検出手段を備えることを特徴とする。

また、本発明は、暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムの情報提供方法において、前記情報提供装置の情報提供方

法は、前記暗号化された情報に、情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第 1 の送信ステップを含み、前記情報配布装置の情報提供方法は、前記情報提供装置から送信された情報の取扱いを示す情報を基に、前記情報の使用料を算出する算出ステップと、前記暗号化された情報に、前記使用料を付加して、前記情報処理装置に送信する第 2 の送信ステップとを含み、前記情報処理装置の情報提供方法は、前記使用料を基に、前記情報の利用に応じた課金情報を作成する課金情報作成ステップと、前記課金情報を、情報の取扱いを示す情報及び使用料の一部又は全部とともに、前記管理装置に送信する第 3 の送信ステップとを含み、前記管理装置の情報提供方法は、前記課金情報、情報の取扱いを示す情報及び使用料の一部又は全部から不正を検出する検出ステップを含むことを特徴とする。

さらに、本発明に係るプログラム提供方法は、暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムの、前記情報提供装置に、前記暗号化された情報に、情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第 1 の送信ステップを含む処理を実行させ、前記情報配布装置に、前記情報提供装置から送信された情報の取扱いを示す情報を基に、前記情報の使用料を算出する算出ステップと、前記暗号化された情報に、前記使用料を付加して、前記情報処理装置に送信する第 2 の送信ステップとを含む処理を実行させ、前記情報処理装置に、前記使用料を基に、前記情報の利用に応じた課金情



報を作成する課金情報作成ステップと、前記課金情報を、情報の取扱いを示す情報及び使用料の一部又は全部とともに、前記管理装置に送信する第3の送信ステップとを含む処理を実行させ、前記管理装置に、前記課金情報、情報の取扱いを示す情報及び使用料の一部又は全部から不正を検出する検出ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

本発明では、暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムにおいて、暗号化された情報に、情報の取扱いを示す情報を付加して、情報配布装置に送信し、受信した暗号化された情報及び情報の取扱いを示す情報を、送信し、情報の取扱いを示す情報を基に、情報の利用に応じた使用許諾情報を作成し、使用許諾情報を、情報の取扱いを示す情報の一部又は全部とともに、送信し、使用許諾情報及び情報の取扱いを示す情報の一部又は全部から不正を検出する。

すなわち、本発明は、暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムにおいて、前記情報提供装置は、前記暗号化された情報に、情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第1の送信手段を備え、前記情報配布装置は、前記情報提供装置から受信した前記暗号化された情報及び前記情報の取扱いを示す

情報を、前記情報処理装置に送信する第 2 の送信手段を備え、前記情報処理装置は、前記情報の取扱いを示す情報を基に、前記情報の利用に応じた使用許諾情報を作成する使用許諾情報作成手段と、前記使用許諾情報を、情報の取扱いを示す情報の一部又は全部とともに、前記管理装置に送信する第 3 の送信手段とを備え、前記管理装置は、前記使用許諾情報及び情報の取扱いを示す情報の一部又は全部から不正を検出する検出手段を備えることを特徴とする。

また、本発明は、暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムの情報提供方法において、前記情報提供装置の情報提供方法は、前記暗号化された情報に、情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第 1 の送信ステップを含み、前記情報配布装置の情報提供方法は、前記情報提供装置から受信した前記暗号化された情報及び前記情報の取扱いを示す情報を、前記情報処理装置に送信する第 2 の送信ステップを含み、前記情報処理装置の情報提供方法は、前記情報の取扱いを示す情報を基に、前記情報の利用に応じた使用許諾情報を作成する使用許諾情報作成ステップと、前記使用許諾情報を、情報の取扱いを示す情報の一部又は全部とともに、前記管理装置に送信する第 3 の送信ステップとを含み、前記管理装置の情報提供方法は、前記使用許諾情報及び情報の取扱いを示す情報の一部又は全部から不正を検出する検出ステップを含むことを特徴とする。

さらに、本発明に係るプログラム提供媒体は、暗号化された情報

を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムの、前記情報提供装置に、前記暗号化された情報に、情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第1の送信ステップを含む処理を実行させ、前記情報配布装置に、前記情報提供装置から受信した前記暗号化された情報及び前記情報の取扱いを示す情報を、前記情報処理装置に送信する第2の送信ステップを含む処理を実行させ、前記情報処理装置に、前記情報の取扱いを示す情報を基に、前記情報の利用に応じた使用許諾情報を作成する使用許諾情報作成ステップと、前記使用許諾情報を、情報の取扱いを示す情報の一部又は全部とともに、前記管理装置に送信する第3の送信ステップとを含む処理を実行させ、前記管理装置に、前記使用許諾情報及び情報の取扱いを示す情報の一部又は全部から不正を検出する検出ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

本発明では、暗号化された情報を提供する情報提供装置及び前記情報を利用する情報処理装置を管理するに当たり、情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録する。

すなわち、本発明は、暗号化された情報を提供する情報提供装置及び前記情報を利用する情報処理装置を管理する管理装置において、前記情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に前記情報処理装置を

登録する登録手段を備えることを特徴とする。

また、本発明は、暗号化された情報を提供する情報提供装置及び前記情報を利用する情報処理装置を管理する管理方法において、前記情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録ステップを含むことを特徴とする。

さらに、本発明に係るプログラム提供媒体は、暗号化された情報を提供する情報提供装置及び前記情報を利用する情報処理装置を管理する管理装置に、前記情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

本発明では、管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置に従属する他の情報処理装置の登録を請求する。

すなわち、本発明は、管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置において、前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求手段を備えることを特徴とする。

また、本発明は、管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置の情報処理方法において、前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップを含むことを特徴とする。

さらに、本発明に係るプログラム提供媒体は、管理装置に登録さ

れ、情報提供装置から提供される暗号化された情報を利用する情報処理装置に、前記情報処理装置に從属する他の情報処理装置の登録を請求する登録請求ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

本発明では、暗号化されて提供される情報を復号し、利用する情報処理装置及び前記情報処理装置を管理する管理装置からなる情報利用システムにおいて、管理装置が、情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録し、情報処理装置が、情報処理装置に從属する他の情報処理装置の登録を請求する。

すなわち、本発明は、暗号化されて提供される情報を復号し、利用する情報処理装置及び前記情報処理装置を管理する管理装置からなる情報利用システムにおいて、前記管理装置は、前記情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録手段を備え、前記情報処理装置は、前記情報処理装置に從属する他の情報処理装置の登録を請求する登録請求手段を備えることを特徴とする。

また、本発明は、管理装置に管理され、かつ、他の情報処理装置と接続され、暗号化された情報を復号し、利用する情報処理装置において、前記管理装置及び前記他の情報処理装置と相互認証する相互認証手段と、所定の情報を復号する復号化手段と、前記管理装置により作成された登録条件を授受する授受手段と、前記授受手段により授受された前記登録条件を記憶する記憶手段と、前記記憶手段により記憶されている前記登録条件に基づいて、動作を制御する制

御手段とを備えることを特徴とする。

また、本発明は、管理装置に管理され、かつ、他の情報処理装置と接続され、暗号化された情報を復号し、利用する情報処理装置の情報処理方法において、前記管理装置及び前記他の情報処理装置と相互認証する相互認証ステップと、所定の情報を復号する復号化ステップと、前記管理装置により作成された登録条件を授受する授受ステップと、前記授受ステップで授受された前記登録条件を記憶する記憶ステップと、前記記憶ステップで記憶された前記登録条件に基づいて、動作を制御する制御ステップとを含むことを特徴とする。

さらに、本発明に係るプログラム提供媒体は、管理装置に管理され、かつ、他の情報処理装置と接続され、暗号化された情報を復号し、利用する情報処理装置に、前記管理装置及び前記他の情報処理装置と相互認証する相互認証ステップと、所定の情報を復号する復号化ステップと、前記管理装置により作成された登録条件を授受する授受ステップと、前記授受ステップで授受された前記登録条件を記憶する記憶ステップと、前記記憶ステップで記憶された前記登録条件に基づいて、動作を制御する制御ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明では、暗号化された情報を復号し、利用する情報処理装置を管理するに当たり、情報処理装置に供給するデータを暗号化し、情報処理装置から、登録条件が送信されてきたとき所定の処理を実行し、所定の処理を実行するときに情報処理装置の登録条件を作成し、作成した登録条件を情報処理装置に送信する。

すなわち、本発明は、暗号化された情報を復号し、利用する情報

処理装置を管理する管理装置において、前記情報処理装置に供給するデータを暗号化する暗号手段と、前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行手段と、前記実行手段により所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成手段と、前記作成手段により作成された前記登録条件を前記情報処理装置に送信する送信手段とを備えることを特徴とする。

また、本発明は、暗号化された情報を復号し、利用する情報処理装置を管理する管理装置の管理方法において、前記情報処理装置に供給するデータを暗号化する暗号ステップと、前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、前記実行ステップで所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成ステップと、前記作成ステップで作成された前記登録条件を前記情報処理装置に送信する送信ステップとを含むことを特徴とする。

さらに、本発明に係るプログラム提供媒体は、暗号化された情報を復号し、利用する情報処理装置を管理する管理装置に、前記情報処理装置に供給するデータを暗号化する暗号ステップと、前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、前記実行ステップで所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成ステップと、前記作成ステップで作成された前記登録条件を前記情報処理装置に送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明では、暗号化されている情報を復号して利用するに

当たり、情報の使用の許諾条件を示す情報を生成し、許諾条件を示す情報の認証情報を生成し、認証情報を記憶する。

すなわち、本発明は、暗号化されている情報を復号して利用する情報処理装置において、前記情報の使用の許諾条件を示す情報を生成する許諾情報生成手段と、前記許諾条件を示す情報の認証情報を生成する認証情報生成手段と、前記認証情報を記憶する記憶手段とを備えることを特徴とする。

また、本発明は、暗号化されている情報を復号して利用する情報処理方法において、前記情報の使用の許諾条件を示す情報を生成する許諾情報生成ステップと、前記許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、前記認証情報を記憶する記憶ステップとを含むことを特徴とする。

さらに、本発明に係るプログラム提供媒体は、暗号化されている情報を復号して利用する情報処理装置に、前記情報の使用の許諾条件を示す情報を生成する許諾情報生成ステップと、前記許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、前記認証情報を記憶する記憶ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明では、装着された情報記憶媒体に情報を記憶させて利用するに当たり、情報の利用のときに必要な関連情報の認証情報を生成し、認証情報を記憶し、関連情報から、他の認証情報を生成し、記憶している認証情報との一致を検証し、情報記憶媒体と相互認証する。

すなわち、本発明は、装着された情報記憶媒体に情報を記憶させて利用する情報処理装置において、前記情報の利用のときに必要な



関連情報の認証情報を生成する認証情報生成手段と、前記認証情報を記憶する記憶手段と、前記関連情報から、他の認証情報を生成し、前記記憶手段が記憶している前記認証情報との一致を検証する検証手段と、前記情報記憶媒体と相互認証する相互認証手段とを備えることを特徴とする。

また、本発明は、装着された情報記憶媒体に情報を記憶させて利用する情報処理装置の情報処理方法において、前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、前記認証情報を記憶する記憶ステップと、前記関連情報から、他の認証情報を生成し、前記記憶ステップで記憶した前記認証情報との一致を検証する検証ステップと、前記情報記憶媒体と相互認証する相互認証ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、装着された情報記憶媒体に情報を記憶させて利用する情報処理装置に、前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、前記認証情報を記憶する記憶ステップと、前記関連情報から、他の認証情報を生成し、前記記憶ステップで記憶した前記認証情報との一致を検証する検証ステップと、前記情報記憶媒体と相互認証する相互認証ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

さらに、本発明は、暗号化された情報を記憶し、情報処理装置に装着される情報記憶媒体において、前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、前記認証情報を記憶する記憶手段と、前記関連情報から、他の認証情報を生成し、前記記憶手段が記憶している前記認証情報との一致を検証する検証

手段と、前記情報処理装置と相互認証する相互認証手段とを備えることを特徴とする。

また、本発明では、情報提供者に代わり、前記情報提供者が提供する情報の利用者から利用料金を徴収し、情報提供者に利益を分配するに当たり、情報を特定するデータ及び情報の利用に対する情報提供者への支払金額を示すデータを記憶し、記憶するデータを基に、情報提供者毎への支払金額の合計を算出し、情報提供者毎の利益を基に、決済機関に対し情報提供者毎の決済を指示する。

すなわち、本発明は、情報提供者に代わり、前記情報提供者が提供する情報の利用者から利用料金を徴収し、情報提供者に利益を分配する情報処理装置において、前記情報を特定するデータ及び前記情報の利用に対する前記情報提供者への支払金額を示すデータを記憶する記憶手段と、前記記憶手段が記憶するデータを基に、前記情報提供者毎への支払金額の合計を算出する算出手段と、前記情報提供者毎の利益を基に、決済機関に対し前記情報提供者毎の決済を指示する決済指示手段とを備えることを特徴とする。

また、本発明は、情報提供者に代わり、前記情報提供者が提供する情報の利用者から利用料金を徴収し、情報提供者に利益を分配する情報処理方法において、前記情報を特定するデータ及び前記情報の利用に対する前記情報提供者への支払金額を示すデータを記憶する記憶ステップと、前記記憶ステップで記憶するデータを基に、前記情報提供者毎への支払金額の合計を算出する算出ステップと、前記情報提供者毎の利益を基に、決済機関に対し前記情報提供者毎の決済を指示する決済指示ステップとを含むことを特

徴とする。

さらに、本発明に係るプログラム提供媒体は、情報提供業者に代わり、前記情報提供業者が提供する情報の利用者から利用料金を徴収し、情報提供業者に利益を分配する情報処理装置に、前記情報を特定するデータ及び前記情報の利用に対する前記情報提供業者への支払金額を示すデータを記憶する記憶ステップと、前記記憶ステップで記憶するデータを基に、前記情報提供業者毎への支払金額の合計を算出する算出ステップと、前記情報提供業者毎の利益を基に、決済機関に対し前記情報提供業者毎の決済を指示する決済指示ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

本発明では、暗号化された情報を復号し、利用するに当たり、情報処理装置を管理する装着された外部記憶媒体と相互認証し、所定の鍵で所定の情報を暗号化する。

すなわち、本発明は、暗号化された情報を復号し、利用する情報処理装置を管理する管理装置において、前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号手段を備えることを特徴とする。

また、本発明は、暗号化された情報を復号し、利用する情報処理装置を管理する管理方法において、前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップを含むことを特徴とする。

さらに、本発明に係るプログラム提供媒体は、暗号化された情報を復号し、利用する情報処理装置を管理する管理装置に、前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する

復号ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

本発明では、装着された外部記憶媒体に所定の情報を記憶させるとともに、暗号化された情報を復号し、利用する情報処理装置及び前記情報処理装置を管理する管理装置からなる情報利用システムにおいて、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する。

すなわち、本発明は、装着された外部記憶媒体に所定の情報を記憶させるとともに、暗号化された情報を復号し、利用する情報処理装置及び前記情報処理装置を管理する管理装置からなる情報利用システムにおいて、前記情報処理装置は、装着された前記外部記憶媒体と相互認証する相互認証手段と、前記管理装置の公開鍵で所定の情報を暗号化する暗号化手段とを備え、前記管理装置は、前記外部記憶媒体に記憶されたデータを復号する復号手段を備えることを特徴とする。

また、本発明は、暗号化された情報を復号し、利用する情報処理装置に装着される外部記憶媒体において、前記情報処理装置と相互認証する相互認証手段を備えることを特徴とする。

#### 図面の簡単な説明

図1は、EMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。

図2は、EMDシステムにおけるEMDサービスセンタの機能構

成を示すブロック図である。

図 3 は、E M D サービスセンタの配送用鍵の送信を説明する図である。

図 4 は、E M D サービスセンタの配送用鍵の送信を説明する図である。

図 5 は、E M D サービスセンタの配送用鍵の送信を説明する図である。

図 6 は、E M D サービスセンタの配送用鍵の送信を説明する図である。

図 7 は、ユーザ登録データベースを説明する図である。

図 8 は、コンテンツプロバイダの機能の構成を示すブロック図である。

図 9 は、サービスプロバイダの機能の構成を示すブロック図である。

図 1 0 は、ユーザホームネットワークの構成を示すブロック図である。

図 1 1 は、ユーザホームネットワークの構成を示すブロック図である。

図 1 2 は、コンテンツ及びコンテンツに付随する情報を説明する図である。

図 1 3 は、コンテンツプロバイダセキュアコンテナを説明する図である。

図 1 4 は、コンテンツプロバイダの証明書を説明する図である。

図 1 5 は、サービスプロバイダセキュアコンテナを説明する図である。

図16は、サービスプロバイダの証明書を説明する図である。

図17(A)，(B)，(C)は、取扱方針、価格情報及び使用許諾情報を示す図である。

図18(A)，(B)は、シングルコピー及びマルチコピーを説明する図である。

図19(A)，(B)，(C)は、取扱方針及び価格情報を説明する図である。

図20(A)，(B)，(C)は、取扱方針、価格情報及び使用許諾情報を説明する図である。

図21は、EMDサービスセンタが、決算処理に必要なデータを収集する動作を説明する図である。

図22は、利益配分データベースの例を示す図である。

図23は、割引テーブルの例を示す図である。

図24は、ユーザ利用料金テーブルの例を示す図である。

図25は、EMDサービスセンタのユーザホームネットワークからの課金情報の受信のときの動作を説明する図である。

図26は、EMDサービスセンタの利益分配処理の動作を説明する図である。

図27は、EMDサービスセンタの、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。

図28は、ユーザホームネットワーク5の更に他の実施の形態の構成を示す図である。

図29は、外部記憶部の記憶の態様を説明する図である。

図30は、記憶モジュールの記憶の態様を説明する図である。

図31は、外部記憶部の他の記憶の態様を説明する図である。

図 3 2 は、記憶モジュールの他の記憶の態様を説明する図である。

図 3 3 は、鍵データの記憶の態様を説明する図である。

図 3 4 は、記憶部の記憶の態様を説明する図である。

図 3 5 は、鍵データの他の記憶の態様を説明する図である。

図 3 6 は、記憶部の他の記憶の態様を説明する図である。

図 3 7 は、コンテンツの配布の処理を説明するフローチャートである。

図 3 8 は、コンテンツの配布の処理を説明するフローチャートである。

図 3 9 は、EMD サービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵を送信する処理を説明するフローチャートである。

図 4 0 は、コンテンツプロバイダと EMD サービスセンタとの相互認証の動作を説明するフローチャートである。

図 4 1 は、コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

図 4 2 は、コンテンツプロバイダと EMD サービスセンタとの相互認証の動作を説明するフローチャートである。

図 4 3 は、レシーバの EMD サービスセンタへの登録の処理を説明するフローチャートである。

図 4 4 は、SAM の証明書を説明する図である。

図 4 5 は、登録リストを説明する図である。

図 4 6 は、IC カードへの SAM のデータのバックアップの処理を説明するフローチャートである。

図 4 7 は、IC カードへの SAM のデータのバックアップの処理を説明するフローチャートである。

図48は、新しいレシーバにICカードのバックアップデータを読み込ませる処理を説明するフローチャートである。

図49は、新しいレシーバにICカードのバックアップデータを読み込ませる処理を説明するフローチャートである。

図50は、新しいレシーバにICカードのバックアップデータを読み込ませる処理を説明するフローチャートである。

図51は、レシーバが、従属関係のあるレコーダをEMDサービスセンタに登録する処理を説明するフローチャートである。

図52は、レシーバがEMDサービスセンタから配送用鍵を受け取る処理を説明するフローチャートである。

図53は、レコーダの配送用鍵の受取処理を説明するフローチャートである。

図54は、コンテンツプロバイダがサービスプロバイダにコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図55は、サービスプロバイダがレシーバにサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図56は、レシーバの課金処理を説明するフローチャートである。

図57は、レシーバの適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を説明するフローチャートである。

図58は、レシーバの適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を説明するフローチャートである。

図59は、レシーバがコンテンツを再生する処理を説明するフローチャートである。

図60は、レシーバがデコーダにコンテンツを再生させる処理を



説明するフローチャートである。

図 6 1 は、E M D サービスセンタの決済オブジェクトを作成する処理を説明するフローチャートである。

図 6 2 (A) , (B) , (C) , (D) は、クレジット決済オブジェクトの例を説明する図である。

図 6 3 (A) , (B) , (C) は、銀行決済オブジェクトの例を説明する図である。

図 6 4 (A) , (B) , (C) , (D) は、クレジット決済オブジェクトの例及び銀行決済オブジェクトの例を説明する図である。

図 6 5 は、クレジット決済処理を説明するフローチャートである。

図 6 6 は、銀行決済処理を説明するフローチャートである。

図 6 7 は、他の E M D システムを説明する図である。

図 6 8 は、登録リストを説明する他の図である。

図 6 9 は、登録リストを説明する他の図である。

図 7 0 は、登録リストを説明する他の図である。

図 7 1 は、登録リストを保持するための処理を説明するフローチャートである。

図 7 2 は、レシーバの登録処理を説明するフローチャートである。

図 7 3 は、登録リストを説明する他の図である。

図 7 4 は、レシーバの登録処理を説明するフローチャートである。

図 7 5 は、登録リストを説明する他の図である。

図 7 6 は、配送用鍵の受取処理を説明するフローチャートである。

図 7 7 は、M D ドライブから供給される暗号化されていないコンテンツを暗号化し、記録する処理の詳細を説明するフローチャートである。

図 7 8 は、レシーバがコンテンツを再生する処理を説明するフローチャートである。

図 7 9 は、レシーバがデコーダにコンテンツを再生させる処理を説明するフローチャートである。

図 8 0 は、レシーバからメモリスティックにコンテンツを移動する処理を説明するフローチャートである。

図 8 1 は、レシーバからメモリスティックにコンテンツを移動する処理を説明するフローチャートである。

図 8 2 は、レシーバからメモリスティックにコンテンツを移動する処理を説明するフローチャートである。

図 8 3 は、レシーバからメモリスティックにコンテンツを移動する処理を説明するフローチャートである。

図 8 4 は、メモリスティックからレシーバにコンテンツを移動する処理を説明するフローチャートである。

図 8 5 は、メモリスティックからレシーバにコンテンツを移動する処理を説明するフローチャートである。

図 8 6 は、メモリスティックからレシーバにコンテンツを移動する処理を説明するフローチャートである。

図 8 7 は、メモリスティックからレシーバにコンテンツを移動する処理を説明するフローチャートである。

図 8 8 は、メモリスティックに記憶されているコンテンツをレシーバが再生する処理を説明するフローチャートである。

図 8 9 は、メモリスティックに記憶されているコンテンツをレシーバ 5 1 が再生する処理を説明するフローチャートである。

発明を実施するための最良の形態

以下、本発明の実施の形態について図面を参照しながら詳細に説明する。

図1は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。このシステムでユーザに配信されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。EMDサービスセンタ1は、コンテンツプロバイダ2、ユーザホームネットワーク5等に配送用鍵Kdを送信し、ユーザホームネットワーク5から、コンテンツの利用に応じた課金情報等を受信し、利用料金を精算し、コンテンツプロバイダ2及びサービスプロバイダ3への利益分配の処理を行う。

コンテンツプロバイダ2は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するためのウォーターマーク（電子透かし）をコンテンツに挿入し、コンテンツを圧縮し、さらに暗号化し、所定の情報を付加して、サービスプロバイダ3に送信する。

サービスプロバイダ3は、専用のケーブルネットワーク、インターネット又は衛星などから構成されるネットワーク4を介して、コンテンツプロバイダ2から供給されたコンテンツに価格を付して、ユーザホームネットワーク5に送信する。

ユーザホームネットワーク5は、サービスプロバイダ3から価格を付して送付されたコンテンツを入手し、コンテンツを復号、再生して利用するとともに課金処理を実行する。課金処理により得られ

た課金情報は、ユーザホームネットワーク 5 が配送用鍵 K d を E M D サービスセンタ 1 から入手する際、E M D サービスセンタ 1 に送信される。

図 2 は、E M D サービスセンタ 1 の機能の構成を示すブロック図である。サービスプロバイダ管理部 1 1 は、サービスプロバイダ 3 に利益分配の情報を供給するとともに、コンテンツプロバイダ 2 から供給されるコンテンツに付される情報（取扱方針）が暗号化されている場合、サービスプロバイダ 3 に配送用鍵 K d を送信する。コンテンツプロバイダ管理部 1 2 は、コンテンツプロバイダ 2 に配送用鍵 K d を送信するとともに、利益分配の情報を供給する。著作権管理部 1 3 は、ユーザホームネットワーク 5 のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、J A S R A C (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) に送信する。鍵サーバ 1 4 は、配送用鍵 K d を記憶しており、コンテンツプロバイダ管理部 1 2 又はユーザ管理部 1 8 等を介して、配送用鍵 K d をコンテンツプロバイダ 2 又はユーザホームネットワーク 5 等に供給する。ユーザ管理部 1 8 は、ユーザホームネットワーク 5 のコンテンツの利用の実績を示す情報である課金情報、そのコンテンツに対応する価格情報及びそのコンテンツに対応する取扱方針を入力し、経歴データ管理部 1 5 に記憶させる。

E M D サービスセンタ 1 からコンテンツプロバイダ 2 及びユーザホームネットワーク 5 を構成するレシーバ 5 1（図 1 0 で後述する）への、配送用鍵 K d の定期的な送信の例について、図 3 乃至図 6 を参照に説明する。図 3 は、コンテンツプロバイダ 2 がコンテン

ツの提供を開始し、ユーザホームネットワーク 5 を構成するレシーバ 5 がコンテンツの利用を開始する、1998 年 1 月における、EMD サービスセンタ 1 が有する配送用鍵 K d、コンテンツプロバイダ 2 が有する配送用鍵 K d 及びレシーバ 5 1 が有する配送用鍵 K d を示す図である。

図 3 の例において、配送用鍵 K d は、暦の月の初日から月の末日まで、使用可能であり、例えば、所定のビット数の乱数である” a a a a a a a ” の値を有するバージョン 1 である配送用鍵 K d は、1998 年 1 月 1 日から 1998 年 1 月 31 日まで使用可能（すなわち、1998 年 1 月 1 日から 1998 年 1 月 31 日の期間にサービスプロバイダ 3 がユーザホームネットワーク 5 に配布するコンテンツを暗号化するコンテンツ鍵 K c o は、バージョン 1 である配送用鍵 K d で暗号化されている）であり、所定のビット数の乱数である” b b b b b b b ” の値を有するバージョン 2 である配送用鍵 K d は、1998 年 2 月 1 日から 1998 年 2 月 28 日まで使用可能（すなわち、その期間にサービスプロバイダ 3 がユーザホームネットワーク 5 に配布するコンテンツを暗号化するコンテンツ鍵 K c o は、バージョン 1 である配送用鍵 K d で暗号化されている）である。同様に、バージョン 3 である配送用鍵 K d は、1998 年 3 月中に使用可能であり、バージョン 4 である配送用鍵 K d は、1998 年 4 月中に使用可能であり、バージョン 5 である配送用鍵 K d は、1998 年 5 月中に使用可能であり、バージョン 6 である配送用鍵 K d は、1998 年 6 月中に使用可能である。

コンテンツプロバイダ 2 がコンテンツの提供を開始するに先立ち、EMD サービスセンタ 1 は、コンテンツプロバイダ 2 に、1998

年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、記憶する。6月分の配送用鍵Kdを記憶するのは、コンテンツプロバイダ2は、コンテンツを提供する前のコンテンツ及びコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、記憶する。3月分の配送用鍵Kdを記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できないなどの事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年2月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2及びレシーバ51への送信を図4で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵Kdを送信し、コンテンツ

プロバイダ 2 は、6 つの配送用鍵 K d を受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、レシーバ 5 1 に、1998 年 2 月から 1998 年 4 月まで、利用可能なバージョン 2 乃至バージョン 4 である 3 つの配送用鍵 K d を送信し、レシーバ 5 1 は、3 つの配送用鍵 K d を受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、バージョン 1 である配送用鍵 K d をそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し又は発見されたときに、過去に利用した配送用鍵 K d を利用できるようにするためである。

1998 年 2 月 1 日から 1998 年 2 月 28 日の期間には、バージョン 2 である配送用鍵 K d が、EMD サービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するレシーバ 5 1 で利用される。

1998 年 3 月 1 日における、EMD サービスセンタ 1 の配送用鍵 K d のコンテンツプロバイダ 2 及びレシーバ 5 1 への送信を図 5 で説明する。EMD サービスセンタ 1 は、コンテンツプロバイダ 2 に、1998 年 3 月から 1998 年 8 月まで利用可能な、バージョン 3 乃至バージョン 8 の 6 つの配送用鍵 K d を送信し、コンテンツプロバイダ 2 は、6 つの配送用鍵 K d を受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、レシーバ 5 1 に、1998 年 3 月から 1998 年 5 月まで、利用可能なバージョン 3 乃至バージョン 5 である 3 つの配送用鍵 K d を送信し、レシーバ 5 1 は、3 つの配送用鍵

K dを受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、バージョン 1 である配送用鍵 K d 及びバージョン 2 である配送用鍵 K d をそのまま記憶する。

1998 年 3 月 1 日から 1998 年 3 月 31 日の期間には、バージョン 3 である配送用鍵 K d が、EMD サービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するレシーバ 51 で利用される。

1998 年 4 月 1 日における、EMD サービスセンタ 1 の配送用鍵 K d のコンテンツプロバイダ 2 及びレシーバ 51 への送信を図 6 で説明する。EMD サービスセンタ 1 は、コンテンツプロバイダ 2 に、1998 年 4 月から 1998 年 9 月まで利用可能な、バージョン 4 乃至バージョン 9 の 6 つの配送用鍵 K d を送信し、コンテンツプロバイダ 2 は、6 つの配送用鍵 K d を受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、レシーバ 51 に、1998 年 4 月から 1998 年 6 月まで、利用可能なバージョン 3 乃至バージョン 5 である 3 つの配送用鍵 K d を送信し、レシーバ 51 は、3 つの配送用鍵 K d を受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、バージョン 1 である配送用鍵 K d、バージョン 2 である配送用鍵 K d 及びバージョン 3 である配送用鍵 K d をそのまま記憶する。

1998 年 4 月 1 日から 1998 年 4 月 30 日の期間には、バージョン 4 である配送用鍵 K d が、EMD サービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するレシー



バ 5 1 で利用される。

このように、あらかじめ先の月の配送用鍵 K d を配布しておくことで、仮にユーザーが 1, 2 か月全くセンターにアクセスしていなくても、一応、コンテンツの買取りが行え、時を見計らって、センターにアクセスして鍵を受信することができる。

利益分配部 1 6 は、経歴データ管理部 1 5 から供給された、課金情報、価格情報及び取扱方針に基づき、E M D サービスセンタ 1、コンテンツプロバイダ 2 及びサービスプロバイダ 3 の利益を算出する。相互認証部 1 7 は、コンテンツプロバイダ 2、サービスプロバイダ 3 及びユーザホームネットワーク 5 の所定の機器と後述する相互認証を実行する。

ユーザ管理部 1 8 は、ユーザ登録データベースを有し、ユーザホームネットワーク 5 の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、又は登録を拒絶するなどの処理を実行する。ユーザホームネットワーク 5 が E M D サービスセンタ 1 と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部 1 8 は、登録が可能か否かの判定の処理の結果に対応して、決済をする機器を指定し、さらに、コンテンツの利用条件を規定した登録リストをユーザホームネットワーク 5 の所定の機器に送信する。

図 7 に示すユーザ登録データベースの例は、ユーザホームネットワーク 5 の機器の機器固有の 6 4 ビットからなる I D (Identification Data) を記録し、その I D に対応して (すなわち、その I D を有する機器毎に)、決済処理が可能か否か、登録が可能か否か、E M D サービスセンタ 1 と接続が可能か否かなどの情報を記録する。

ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関（例えば、銀行）又はサービスプロバイダ3などから供給される料金の未払、不正処理等の情報を基に、所定の時間間隔で更新される。登録が不可と記録されたIDを有する機器の登録の要求に対して、ユーザ管理部18は、その登録を拒否し、登録を拒否された機器は、以後、このシステムのコンテンツを利用できない。

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク5が、コンテンツの再生又はコピーなどの利用が可能な複数の機器で構成されているとき、その中の決済処理が可能である1台の機器は、EMDサービスセンタ1に、ユーザホームネットワーク5のEMDサービスセンタ1に登録されているすべての機器の、課金情報、価格情報及び取扱方針を出力する。ユーザ登録データベースに記録されたEMDサービスセンタ1と接続が可能か否かの情報は、その機器が、EMDサービスセンタ1と接続が可能であるか否かを示し、接続ができないと記録された機器は、ユーザホームネットワーク5の他の機器を介して、EMDサービスセンタ1に、課金情報等を出力する。

また、ユーザ管理部18は、ユーザホームネットワーク5の機器から課金情報、価格情報及び取扱方針が供給され、その情報を経歴データ管理部15に出力し、さらに、所定の処理（タイミング）で、ユーザホームネットワーク5の機器に、配送用鍵Kdを供給する。

課金請求部19は、経歴データ管理部15から供給された、課金情報、価格情報及び取扱方針に基づき、ユーザへの課金を算出し、その結果を出納部20に供給する。出納部20は、ユーザ、コンテ

コンテンツプロバイダ2及びサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、価格情報及び取扱方針の正当性（すなわち、不正をしていないか）を監査する。

図8は、コンテンツプロバイダ2の機能の構成を示すブロック図である。コンテンツサーバ31は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部32に供給する。ウォーターマーク付加部32は、コンテンツサーバ31から供給されたコンテンツにウォーターマークを付加し、圧縮部33に供給する。圧縮部33は、ウォーターマーク付加部32から供給されたコンテンツを、A T R A C (Adaptive Transform Acoustic Coding 2) (商標)などの方式で圧縮し、暗号化部34に供給する。暗号化部34は、圧縮部33で圧縮されたコンテンツを、乱数発生部35から供給された乱数を鍵（以下、この乱数をコンテンツ鍵K<sub>co</sub>と称する）として、D E S (Data Encryption Standard)などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテンツ作成部38に出力する。

なお、この実施の形態においては、コンテンツはA T R A C方式で圧縮されるものとして説明するが、これに限られるものではなく、コンテンツが音楽などである場合にはA C C (Advanced Audio Coding)、M P 3 (MPEG-1 Audio Layer3)など、また、コンテンツが画像などである場合には、M P E G (Moving Picture Experts Group)、J P E G (Joint Photographic Coding Experts Group)などの圧縮が行われ、圧縮方式にはこだわらない。

乱数発生部35は、コンテンツ鍵K<sub>co</sub>となる所定のビット数の

乱数を暗号化部 34 及び暗号化部 36 に供給する。暗号化部 36 は、コンテンツ鍵 K<sub>co</sub>を EMD サービスセンタ 1 から供給された配送用鍵 K<sub>d</sub>を使用して、DES などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

DES は、56 ビットの共通鍵を用い、平文の 64 ビットを 1 ブロックとして処理する暗号方式である。DES の処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DES のすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文の 64 ビットは、上位 32 ビットの H<sub>0</sub> 及び下位 32 ビットの L<sub>0</sub> に分割される。鍵処理部から供給された 48 ビットの拡大鍵 K<sub>1</sub> 及び下位 32 ビットの L<sub>0</sub> を入力とし、下位 32 ビットの L<sub>0</sub> を攪拌した F 関数の出力が算出される。F 関数は、数値を所定の規則で置き換える「換字」及びビット位置を所定の規則で入れ替える「転置」の 2 種類の基本変換から構成されている。次に、上位 32 ビットの H<sub>0</sub> と、F 関数の出力が排他的論理和され、その結果は L<sub>1</sub> とされる。L<sub>0</sub> は、H<sub>1</sub> とされる。

上位 32 ビットの H<sub>0</sub> 及び下位 32 ビットの L<sub>0</sub> を基に、以上の処理を 16 回繰り返し、得られた上位 32 ビットの H<sub>16</sub> 及び下位 32 ビットの L<sub>16</sub> が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆に辿ることで実現される。

ポリシー記憶部 37 は、コンテンツの取扱方針（ポリシー）を記憶し、暗号化されるコンテンツに対応して、取扱方針をセキュアコンテナ作成部 38 に出力する。セキュアコンテナ作成部 38 は、暗

号化されたコンテンツ、暗号化されたコンテンツ鍵  $K_{co}$ 、取扱方針並びにこれらデータのハッシュ値をとり作成された署名、さらにコンテンツプロバイダ 2 の公開鍵  $K_{cp}$  を含む証明書から構成されるコンテンツプロバイダセキュアコンテナを作成し、サービスプロバイダ 3 に供給する。相互認証部 39 は、EMD サービスセンタ 1 から配送用鍵  $K_d$  の供給を受けるのに先立ち、EMD サービスセンタ 1 と相互認証し、また、サービスプロバイダ 3 へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ 3 と相互認証する。

署名は、データ又は後述する証明書に付け、改竄のチェック及び作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

ハッシュ関数及び署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの 1 ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された

場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD 4，MD 5，SHA-1などが用いられる。

次に公開鍵暗号について説明する。暗号化及び復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

公開鍵暗号の中で代表的なRSA(Rivest-Shamir-Adleman)暗号を、簡単に説明する。まず、2つの十分に大きな素数である $p$ 及び $q$ を求め、さらに $p$ と $q$ の積である $n$ を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 $L$ を算出し、さらに、3以上 $L$ 未満で、かつ、 $L$ と互いに素な数 $e$ を求める（すなわち、 $e$ と $L$ を共通に割り切れる数は、1のみである）。

次に、 $L$ を法とする乗算に関する $e$ の乗法逆元 $d$ を求める。すなわち、 $d$ 、 $e$ 及び $L$ の間には、 $ed = 1 \pmod{L}$ が成立し、 $d$ はユークリッドの互除法で算出できる。このとき、 $n$ と $e$ が公開鍵とされ、 $p$ 、 $q$ 及び $d$ が、秘密鍵とされる。

暗号文 $C$ は、平文 $M$ から、式(1)の処理で算出される。

$$C = M^e \pmod{n} \quad (1)$$

暗号文 $C$ は、式(2)の処理で平文 $M$ に、復号される。

$$M = C^d \pmod{n} \quad (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それ

が復号できるのは、フェルマーの小定理に根拠をおいており、式  
(3) が成立するからである。

$$M = C^d = (M^e)^d = M^{(ed)} \bmod n \quad (3)$$

秘密鍵  $p$  と  $q$  を知っているならば、公開鍵  $e$  から秘密鍵  $d$  は算出できるが、公開鍵  $n$  の素因数分解が計算量的に困難な程度に公開鍵  $n$  の桁数を大きくすれば、公開鍵  $n$  を知るだけでは、公開鍵  $e$  から秘密鍵  $d$  は計算できず、復号できない。以上のように、RSA 暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができ。

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線  $y^2 = x^3 + ax + b$  上の、ある点を  $B$  とする。楕円曲線上の点の加算を定義し、 $nB$  は、 $B$  を  $n$  回加算した結果を表す。同様に、減算も定義する。 $B$  と  $nB$  から  $n$  を算出することは、困難であることが証明されている。 $B$  と  $nB$  を公開鍵とし、 $n$  を秘密鍵とする。乱数  $r$  を用いて、暗号文  $C1$  及び  $C2$  は、平文  $M$  から、公開鍵で式 (4) 及び式 (5) の処理で算出される。

$$C1 = M + r n B \quad (4)$$

$$C2 = r B \quad (5)$$

暗号文  $C1$  及び  $C2$  は、式 (6) の処理で平文  $M$  に、復号される。

$$M = C1 - n C2 \quad (6)$$

復号できるのは、秘密鍵  $n$  を有するものだけである。以上のように、RSA 暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

図9は、サービスプロバイダ3の機能の構成を示すブロック図である。コンテンツサーバ41は、コンテンツプロバイダ2から供給

された、暗号化されているコンテンツを記憶し、セキュアコンテナ作成部 4 4 に供給する。値付け部 4 2 は、コンテンツに対応した取扱方針を基に、価格情報を作成し、セキュアコンテナ作成部 4 4 に供給する。ポリシー記憶部 4 3 は、コンテンツプロバイダ 2 から供給された、コンテンツの取扱方針を記憶し、セキュアコンテナ作成部 4 4 に供給する。相互認証部 4 5 は、コンテンツプロバイダ 2 からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ 2 と相互認証し、また、ユーザホームネットワーク 5 へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク 5 と相互認証する。また、コンテンツプロバイダ 2 が取り扱い方針を配送用鍵 K d で暗号化して供給する場合、相互認証部 4 5 は、E M D サービスセンタ 1 から配送用鍵 K d の供給を受け付けるのに先立ち、E M D サービスセンタ 1 と相互認証する。

図 1 0 は、ユーザホームネットワーク 5 の構成を示すブロック図である。レシーバ 5 1 は、ネットワーク 4 を介して、サービスプロバイダ 3 からコンテンツを含んだサービスプロバイダセキュアコンテナを受信し、コンテンツを復号及び伸張し、再生する。

通信部 6 1 は、ネットワーク 4 を介してサービスプロバイダ 3、又は E M D サービスセンタ 1 と通信し、所定の情報を受信し又は送信する。S A M (Secure Application Module) 6 2 は、サービスプロバイダ 3 又は E M D サービスセンタ 1 と相互認証し、暗号化されているコンテンツを復号し又はコンテンツを暗号化し、さらに配送用鍵 K d 等を記憶する。伸張部 6 3 は、暗号化されているコンテンツを復号し、A T R A C 方式で伸張し、さらに所定のウォーターマー



クをコンテンツに挿入する。I C(Integrated Circuit)カードインターフェース 6 4 は、S A M 6 2 からの信号を所定の形式に変更し、レシーバ 5 1 に装着された I C カード 5 5 に出力し、また、I C カード 5 5 からの信号を所定の形式に変更し、S A M 6 2 に出力する。

サービスプロバイダ 3 又は E M D サービスセンタ 1 と相互認証し、課金処理を実行し、コンテンツ鍵 K c o を復号及び暗号化し、さらに使用許諾情報等の所定のデータを記憶する S A M 6 2 は、相互認証モジュール 7 1、課金モジュール 7 2、記憶モジュール 7 3 及び復号／暗号化モジュール 7 4 から構成される。この S A M 6 2 は、シングルチップの暗号処理専用 I C で構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧又は周波数の幅が狭いなど、外部から不正にデータが読み出し難い特性（耐タンパー性）を有する。

相互認証モジュール 7 1 は、サービスプロバイダ 3 又は E M D サービスセンタ 1 との相互認証を実行し、必要に応じて、一時鍵 K t e m p（セッション鍵）を復号／暗号化モジュール 7 4 に供給する。課金処理モジュール 7 2 は、サービスプロバイダ 3 から受信したサービスプロバイダセキュアコンテナに含まれる取扱方針及び価格情報から、使用許諾情報及び課金情報を生成し、記憶モジュール 7 3 又は H D D(Hard Disk Drive) 5 2 に出力する。記憶モジュール 7 3 は、課金処理モジュール 7 2 又は復号／暗号化モジュール 7 4 から供給された課金情報及び配送用鍵 K d 等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送用鍵 K d 等のデータを供給する。

復号／暗号化モジュール 7 4 は、復号ユニット 9 1、乱数発生ユ

ニット 9 2 及び暗号化ユニット 9 3 から構成される。復号ユニット 9 1 は、暗号化されたコンテンツ鍵  $K_{co}$  を配送用鍵  $K_d$  で復号し、暗号化ユニット 9 3 に出力する。乱数発生ユニット 9 2 は、所定の桁数の乱数を発生し、保存用鍵  $K_{save}$  として暗号化ユニット 9 3 及び記憶モジュール 7 3 に出力する。ただし、一度生成して保持している場合、生成の必要はない。暗号化ユニット 9 3 は、復号されたコンテンツ鍵  $K_{co}$  を、再度、保存用鍵  $K_{save}$  で暗号化し、HDD 5 2 に出力する。暗号化ユニット 9 3 は、コンテンツ鍵  $K_{co}$  を伸張部 6 3 に送信するとき、コンテンツ鍵  $K_{co}$  を一時鍵  $K_{temp}$  で暗号化する。

コンテンツを復号し、伸張し、所定のウォータマークを付加する伸張部 6 3 は、相互認証モジュール 7 5、復号モジュール 7 6、伸張モジュール 7 8 及びウォータマーク付加モジュール 7 9 から構成される。相互認証モジュール 7 5 は、SAM 6 2 と相互認証し、一時鍵  $K_{temp}$  を復号モジュール 7 6 に出力する。復号モジュール 7 6 は、SAM 6 2 から出力され、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_{co}$  を一時鍵  $K_{temp}$  で復号する。さらに、復号モジュール 7 6 は、HDD 5 2 に記録されたコンテンツをコンテンツ鍵  $K_{co}$  で復号し、伸張モジュール 7 8 に出力する。伸張モジュール 7 8 は、復号されたコンテンツを、更に ATRAC 等の方式で伸張し、ウォータマーク付加モジュール 7 9 に出力する。ウォータマーク付加モジュール 7 9 は、コンテンツにレシーバ 5 1 を特定する所定のウォータマークを挿入し、レコーダ 5 3 に出力したり、図示せぬスピーカに出力し、音楽を再生する。

HDD 5 2 は、サービスプロバイダ 3 から供給されたコンテンツ

を記録する。図10ではレシーバ51、HDD52は独立して存在するように記載してあるが勿論これらは一体形成されていても良い。装着された光ディスク（図示せず）にサービスプロバイダ3から供給されたコンテンツを記録し、再生するレコーダ53は、記録再生部65、SAM66及び伸張部67から構成される。記録再生部65は、光ディスクが装着され、その光ディスクにコンテンツを記録し、再生する。SAM66は、SAM62と同じ機能を有し、その説明は省略する。伸張部67は、伸張部63と同じ機能を有し、その説明は省略する。MD(Mini Disk：商標)ドライブ54は、装着された図示せぬMDにサービスプロバイダ3から供給されたコンテンツを記録し、再生する。

ICカード55は、レシーバ51に装着され、記憶モジュール73に記憶された配送用鍵Kd及び機器のIDなどの所定のデータを記憶する。例えば、新たなレシーバ51を購入し、今まで使用していたレシーバ51と入れ替えて使用する場合、まず、ユーザは、ICカード55に、今まで使用していたレシーバ51の記憶モジュール73に記憶されていた配送用鍵Kdなどの所定のデータを記憶させる。次に、ユーザは、そのICカード55を新たなレシーバ51に装着し、そのレシーバ51を操作して、EMDサービスセンタ1のユーザ管理部18にその新たなレシーバ51を登録する。EMDサービスセンタ1のユーザ管理部18は、ICカード55に記憶されていたデータ（今まで使用していたレシーバ51のIDなど）基に、ユーザ管理部18が保持しているデータベースから、ユーザの氏名、使用料の払込みに使用するクレジットカードの番号などのデータを検索し、そのデータを基に、登録の処理を実行するので、ユ

一ザは、面倒なデータを入力する必要がない。ICカード55は、相互認証モジュール80及び記憶モジュール81で構成される。相互認証モジュール80は、SAM62と相互認証する。記憶モジュール81は、ICカードインターフェース64を介して、SAM62から供給されたデータを記憶し、記憶したデータをSAM62に出力する。

図11は、ユーザホームネットワーク5の他の構成例を示すブロック図である。この構成のレシーバ51及びレコーダ53は、図10に示したレシーバ51の伸張部63及びレシーバ53の伸張部67を省略した構成を有する。その代わり、レコーダ53に接続されているデコーダ56が、伸張部63又は伸張部67と同じ機能を有する。その他の構成は、図10における場合と同様である。

コンテンツを復号し、伸張し、ウォータマークを付加するデコーダ56は、相互認証モジュール101、復号モジュール102、復号モジュール103、伸張モジュール104及びウォータマーク付加モジュール105から構成される。相互認証モジュール101は、SAM62又はSAM66と相互認証し、一時鍵Ktempを復号モジュール102に出力する。復号モジュール102は、SAM62から出力され、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを一時鍵Ktempで復号し、復号モジュール103に出力する。復号モジュール103は、HDD52に記録されたコンテンツをコンテンツ鍵Kcoで復号し、伸張モジュール104に出力する。伸張モジュール104は、復号されたコンテンツを、更にATRA C等の方式で伸張し、ウォータマーク付加モジュール105に出力する。ウォータマーク付加モジュール105は、コンテンツにデコ

ータ56を特定する所定のウォータマークを挿入し、レコーダ53に出力したり、図示せぬスピーカに出力し、音楽を再生する。

図12は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3及びユーザホームネットワーク5の間で送受信される情報を説明する図である。コンテンツプロバイダ2は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K<sub>co</sub>、取扱方針及び署名をコンテンツプロバイダセキュアコンテナ（その詳細は図13を参照して後述する）に格納し、さらにコンテンツプロバイダセキュアコンテナにコンテンツプロバイダ2の証明書（その詳細は図14を参照して後述する）を付して、サービスプロバイダ3に送信する。コンテンツプロバイダ2はまた、必要に応じて取扱方針及び署名にコンテンツプロバイダ2の証明書を付して、EMDサービスセンタ1に送信する。

サービスプロバイダ3は、受信したコンテンツプロバイダ2の証明書を検証し、コンテンツプロバイダ2の公開鍵K<sub>pcp</sub>を入手し、受信したコンテンツプロバイダセキュアコンテナの署名を検証する。署名の検証に成功した後、コンテンツプロバイダセキュアコンテナから取扱方針を取り出し、これを基に価格情報を生成する。サービスプロバイダ3は、さらに、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K<sub>co</sub>、取扱方針、価格情報及び署名をサービスプロバイダセキュアコンテナ（その詳細は図15を参照して後述する）に格納し、さらに、サービスプロバイダセキュアコンテナにサービスプロバイダ3の証明書（その詳細は図16を参照して後述する）を付して、ユーザホームネットワーク5に送信する。サービスプロバイダ3は、また、価格情報及び署名にサービスプロバイダ3

の証明書を付して、E M D サービスセンタ 1 に送信する。

ユーザホームネットワーク 5 は、受信したサービスプロバイダセキュアコンテナを検証した後、セキュアコンテナに含まれる取扱方針及び価格情報に基づいて購入処理を行う。ユーザホームネットワーク 5 は、取扱方針の中から購入形態を選択し、携帯使用許諾情報を生成し、それに応じた課金情報を生成して S A M 内の記憶モジュールに保存する。使用許諾情報は、暗号化されているコンテンツ、復号されてレシーバの保存鍵 K s a v e で再暗号化されたコンテンツ鍵 K c o とともに、レシーバの外部メモリに保存される。課金情報は、所定のタイミングで、暗号化され署名が付され、必要に応じて取扱方針及び価格情報とともに E M D サービスセンタ 1 に送信される。

E M D サービスセンタ 1 は、課金情報及び価格情報を基に使用料金を算出し、また E M D サービスセンタ 1、コンテンツプロバイダ 2 及びサービスプロバイダ 3 それぞれの利益を算出する。E M D サービスセンタ 1 は、さらに、コンテンツプロバイダ 2 から受信した取扱方針、サービスプロバイダ 3 から受信した価格情報並びにユーザホームネットワーク 5 から受信した課金情報及び取扱方針を比較し、サービスプロバイダ 3 又はユーザホームネットワーク 5 で取り扱い方針の改竄又は不正な価格の付加等の不正がなかったか否かを監査する。なお、図 1 2 においては、取扱方針、価格情報は暗号化されずに伝送しているが、これに限らず暗号化して伝送しても良い。むしろ暗号化した方がシステムの外部からの攻撃に対し安全性が向上する。

図 1 3 は、コンテンツプロバイダセキュアコンテナを説明する図

である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、配送用鍵  $K_d$  で暗号化されたコンテンツ鍵  $K_{co}$ 、取扱方針及び署名を含む。署名は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、配送用鍵  $K_d$  で暗号化されたコンテンツ鍵  $K_{co}$  及び取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ 2 の秘密鍵  $K_{scp}$  で暗号化したデータである。

図 14 は、コンテンツプロバイダ 2 の証明書を説明する図である。コンテンツプロバイダ 2 の証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズム及びパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ 2 の名前、コンテンツプロバイダの公開鍵  $K_{pcp}$  並びに署名を含む。署名は、証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズム及びパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ 2 の名前並びにコンテンツプロバイダの公開鍵  $K_{pcp}$  にハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵  $K_{sca}$  で暗号化したデータである。

図 15 は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、配送用鍵  $K_d$  で暗号化されたコンテンツ鍵  $K_{co}$ 、取扱方針、価格情報及び署名を含む。署名は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、配送用鍵  $K_d$  で暗号化されたコンテンツ鍵  $K_{co}$ 、取扱方針及び価格情報にハッシュ関数

を適用して生成されたハッシュ値を、サービスプロバイダ3の秘密鍵  $K_{sps}$  で暗号化したデータである。

図16は、サービスプロバイダ3の証明書を説明する図である。サービスプロバイダ3の証明書は、証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける証明書の通し番号、署名に用いたアルゴリズム及びパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダの公開鍵  $K_{psp}$  並びに署名を含む。署名は、証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける証明書の通し番号、署名に用いたアルゴリズム及びパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダの公開鍵  $K_{psp}$  にハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵  $K_{sca}$  で暗号化したデータである。

図17(A)、(B)、(C)は、取扱方針、価格情報及び使用許諾情報を示す図である。コンテンツプロバイダ2が有する取扱方針(図17(A))は、コンテンツ毎に用意され、ユーザホームネットワーク5が利用可能な利用内容を示す。例えば、図17(A)の取扱方針は、ユーザホームネットワーク5がそのコンテンツを再生及びマルチコピーすることは許可するが、シングルコピーは許可しないことを示す。

図18(A)、(B)は、シングルコピー及びマルチコピーを説明する図である。マルチコピーは、使用許諾情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、複数のコピーを作成することを言う。ただし、図18(A)に示すように、コピーを更にコピ



一することはできない（許されない）。シングルコピーは、使用許諾情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、ただ1つのコピーを作成することを言う。シングルコピーの場合も、図18（B）に示すように、コピーを更にコピーすることはできない（許されない）。

サービスプロバイダ3は、図17（B）に示すように、コンテンツプロバイダ2からの取扱方針（図17（A））に価格情報を加える。例えば、図17（B）の価格情報は、そのコンテンツを再生して利用するときの料金が150円で、マルチコピーして利用するときの利用料金が80円であることを示す。図17には、例示しないが、シングルコピーの価格情報は、コピーの1回当たりの使用料金を表し、例えば、3回のコピーの利用では、シングルコピーの使用料金の3倍の料金を支払う。マルチコピー又はシングルコピーが許可されるコンテンツは、使用許諾情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合における、そのコンテンツに限られる。

ユーザホームネットワーク5は、サービスプロバイダ3から供給される取扱方針が示すコンテンツの利用可能な利用内容（図17（B））から、ユーザが選択した、利用内容を示す使用許諾情報（図17（C））を記憶する。例えば、図17（C）の使用許諾情報は、そのコンテンツを再生して使用することができ、シングルコピー及びマルチコピーができないことを示す。

図19（A），（B），（C）は、図17（A），（B），（C）の例と比較してコンテンツプロバイダ2が取り扱い方針に利

益分配の情報を加え、サービスプロバイダ 3 が価格情報に利益分配の情報を加える場合の、取扱方針及び価格情報を説明する図である。図 17 (A), (B), (C) に示す例に対して、図 19 (A), (B), (C) の例では、コンテンツプロバイダ 2 の利益が、コンテンツを再生して利用するとき 70 円で、マルチコピーして利用するとき 40 円であることを示す情報が、追加されている (図 19 (A))。さらに、利益分配情報として、サービスプロバイダ 3 の利益が、コンテンツを再生して利用するとき 60 円で、マルチコピーして利用するとき 30 円であることが、追加されている (図 19 (B))。価格は、図 17 (A) における場合と同様に、再生が 150 円、マルチコピーが 80 円とされている。価格 (例えば 150 円) からコンテンツプロバイダ 2 の利益 (例えば 70 円) 及びサービスプロバイダ 3 の利益 (例えば 60 円) を差し引いた金額 (例えば 20 円) が、EMD サービスセンタ 1 の利益である。EMD サービスセンタ 1 は、ユーザホームネットワーク 5 のコンテンツの利用結果を示す課金情報 (図 19 (C)) とともに、ユーザホームネットワーク 5 を介して、取扱方針、利益分配率及び価格情報を得ることで、コンテンツプロバイダ 2、サービスプロバイダ 3 及び EMD サービスセンタ 1 のそれぞれの利益を算出できる。

図 20 (A), (B), (C) は、コンテンツの再生の利用に、複数の形態が設定されているときの取扱方針、価格情報及び使用許諾情報を説明する図である。図 20 (A) の例では、サービスプロバイダ 3 において、取扱方針及び価格情報として、コンテンツの再生利用に、制限のない再生、回数制限 (この例の場合、5 回) のある再生及び期間制限 (この例の場合、1998 年 12 月 31 日ま

で)のある再生が設定されている。ユーザが、5回の回数制限のある再生を選択して、コンテンツを利用する場合、コンテンツを受け取り、まだ1度も再生していない状態では、図20(B)に示すように、ユーザホームネットワーク5の使用許諾情報の回数制限に対応する値には、“5”が記録されている。この回数制限に対応する値は、ユーザホームネットワーク5において、コンテンツが再生(利用)されるたびにデクリメントされ、例えば、3回再生された後、その値は、図20(C)に示すように“2”とされる。回数制限に対応する値が、“0”となった場合、ユーザホームネットワーク5は、それ以上、そのコンテンツを再生して利用することができない。

図21は、EMDサービスセンタ1が、コンテンツプロバイダ2、サービスプロバイダ3及びユーザホームネットワーク5から、決算処理に必要なデータを収集する他の動作を説明する図である。コンテンツプロバイダ2は、EMDサービスセンタ1に、コンテンツプロバイダ2の名前、コンテンツID、コンテンツIDに対応する権利団体の利益及びコンテンツプロバイダ2の銀行口座番号などのデータからなるコンテンツプロバイダ登録データを送信し、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、コンテンツプロバイダ登録データを受信する。EMDサービスセンタ1のコンテンツプロバイダ管理部12は、コンテンツプロバイダ登録データを受信したとき、コンテンツプロバイダIDを生成し、コンテンツプロバイダIDとともにコンテンツプロバイダ登録データを利益配分データベースに登録し、コンテンツプロバイダIDをコンテンツプロバイダ2に送信する。コンテンツプロバイダ2は、コンテン

プロバイダ I D を受信し、記憶する。

サービスプロバイダ 3 は、E M D サービスセンタ 1 にサービスプロバイダ 3 の名前、コンテンツ I D 及びサービスプロバイダ 3 の銀行口座番号などのデータからなるサービスプロバイダ登録データを送信し、E M D サービスセンタ 1 のサービスプロバイダ管理部 1 1 は、サービスプロバイダ登録データを受信する。E M D サービスセンタ 1 のサービスプロバイダ管理部 1 1 は、サービスプロバイダ登録データを受信したとき、サービスプロバイダ I D を生成し、サービスプロバイダ I D をサービスプロバイダ 3 に送信する。サービスプロバイダ 3 は、コンテンツプロバイダ I D を受信し、記憶する。

ユーザホームネットワーク 5 は、E M D サービスセンタ 1 にユーザの名前、ユーザの銀行口座番号などのデータからなるユーザ登録データを送信し、E M D サービスセンタ 1 のユーザ管理部 1 8 は、ユーザ登録データを受信する。E M D サービスセンタ 1 のユーザ管理部 1 8 は、ユーザ登録データの受信により、ユーザ I D を生成し、ユーザ I D とともにユーザ登録データを記憶し、ユーザ I D をユーザホームネットワーク 5 に送信する。ユーザホームネットワーク 5 は、ユーザ I D を受信し、記憶する。

図 2 2 は、E M D サービスセンタ 1 の利益配分部 1 6 が保持する利益配分データベースの例を示す図である。利益配分データベースは、コンテンツ I D に対応する権利団体への利益配分を示すデータが記憶されている。コンテンツ I D に対応する権利団体への利益配分を示すデータは、権利団体への、コンテンツ I D に対応するコンテンツがユーザに利用されたときに発生する利益の配分の割合を示す。

図 2 2 に示す利益配分データベースの例において、コンテンツ ID が 1 であるコンテンツがサービスプロバイダ 3 からユーザに提供された場合、権利団体には、コンテンツがユーザに利用されることによる利益の 10 % が配分される。同様に、コンテンツ ID が 2 であるコンテンツがユーザに利用されることによる利益の 20 % は、権利団体に配分される。

図 2 3 は、EMD サービスセンタ 1 の利益分配部 1 6 が記憶するコンテンツの利用料金の割引テーブルの例を示す図である。コンテンツの利用料金の割引テーブルには、コンテンツ ID 及びコンテンツプロバイダ ID に対応するユーザの利用料金の割引率が格納されている。割引テーブルには、割引率を、適用する期間の情報なども格納できるようになされている。

コンテンツプロバイダ ID が 1 であるコンテンツプロバイダ 2 が供給するコンテンツ ID が 1 であるコンテンツの利用料金は、1998 年 9 月から 1998 年 12 月までの間、2 % 割り引かれる。コンテンツプロバイダ ID が 1 であるコンテンツプロバイダ 2 が供給するコンテンツ ID が 2 であるコンテンツの利用料金は、3 % 割り引かれる。コンテンツプロバイダ ID が 1 であるコンテンツプロバイダ 2 が供給するコンテンツ ID が 1 又は 2 以外であるコンテンツの利用料金は、1 % 割り引かれる。コンテンツプロバイダ ID が 2 であるコンテンツプロバイダ 2 が供給するコンテンツ ID が 3 であるコンテンツの利用料金は、5 % 割り引かれる。サービスプロバイダ ID が 1 であるサービスプロバイダ 3 が提供するコンテンツ ID が 1 であるコンテンツの利用料金は、3 % 割り引かれる。サービスプロバイダ ID が 2 であるサービスプロバイダ 3 が提供するコンテ

ンツIDが4であるコンテンツの利用料金は、1%割引かれる。

図24は、EMDサービスセンタ1の課金請求部19が記憶する、ユーザに対するEMDサービスセンタ1の利用料金を格納するユーザ利用料金テーブルの例を示している。ユーザ利用料金テーブルの月額固定額は、ユーザがEMDサービスセンタ1に毎月支払う一定の利用料金の額を表す。変動額は、EMDサービスセンタ1が特別に定めた所定の期間の月額固定額の割引率又はコンテンツの利用料金を含めた利用料が所定の額以上である場合の月額固定額の割引率を表す。

図24に示すユーザ利用料金テーブルの例において、月額固定額は、1000円であり、1998年8月から1998年9月の間、月額固定額は、10%割引かれる。また、コンテンツの利用料金を含めた利用料が3000円以上である場合、月額固定額は、5%割引かれる。

利益配分データベース又は課金情報からコンテンツの利用料金が算出され、コンテンツの利用料金から割引テーブルに基づく割引額が減算され、ユーザ利用料金テーブルに格納されているEMDサービスセンタ1の利用料金が加算されて、ユーザの利用料金が、算出される。

図25は、EMDサービスセンタ1が、ユーザホームネットワーク5から課金情報を受信するときの動作を説明する図である。EMDサービスセンタ1の相互認証部17は、ユーザホームネットワーク5と相互認証した後、一時鍵Ktempを共有する。ユーザホームネットワーク5は、共有した一時鍵Ktempを用いて課金情報、必要に応じて取扱方針等を暗号化し、署名データを付加してEMD

サービスセンタ 1 に送信する。E M D サービスセンタ 1 のユーザ管理部 1 8 は、受信した署名データを検証し、改竄がなければ、共有した一時鍵 K t e m p で受信した課金情報等を復号し、経歴データ管理部 1 5 に送信する。

ユーザ管理部 1 8 は、鍵サーバ 1 4 からの配送用鍵 K d を受信し、これを共有した一時鍵 K t e m p で暗号化して署名データを付加し、ユーザ登録データベースから登録情報を作成し、一時鍵 K t e m p で暗号化された配送用鍵 K d、署名データ及び登録情報をユーザホームネットワーク 5 内の決済可能機器に送信する。登録情報の作成については、図 7 で説明した通りであり、ここでの詳細説明は省略する。

経歴データ管理部 1 5 は、決済を実行すると判定した場合、受信した課金情報を利益分配部 1 6 に送信し、さらに、受信した課金情報及び取扱方針等を課金請求部 1 9 に送信する。利益分配部 1 6 は、コンテンツプロバイダ 2、サービスプロバイダ 3 及び E M D サービスセンタ 1 自身に対する請求金額及び支払金額を算出する。課金請求部 1 9 は、ユーザの支払金額を算出し、その情報を出納部 2 0 に送信する。出納部 2 0 は、図示せぬ外部の銀行等と通信し、決算処理を実行する。その際、ユーザの未払料金等の情報があれば、それらの情報は決済報告の形で課金請求部 1 9 及びユーザ管理部 1 8 に送信され、ユーザ登録データベースに反映され、以降のユーザ登録処理又は決済処理時に参照される。

一時鍵 K t e m p で暗号化され署名データを付された配送用鍵 K d 及び登録情報を受信したユーザホームネットワーク 5 内の決済可能機器は、記憶してあった登録情報を更新するとともに、署名デー

タを検証した後、配送用鍵K dを一時鍵K t e m pで復号し、暗号処理部内の記憶モジュールに記憶されている配送用鍵K dを更新し、記憶モジュール内の課金情報を削除する。

図26は、EMDサービスセンタ1の利益分配処理の動作を説明する図である。経歴データ管理部15は、ユーザのコンテンツの使用実績を示す課金情報、取扱方針及び価格情報を利益分配部16に送信する。利益分配部16は、これらの情報を基に、コンテンツプロバイダ2、サービスプロバイダ3及びEMDサービスセンタ1それぞれの利益を算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、出納部20及び著作権管理部13に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。サービスプロバイダ管理部11は、サービスプロバイダ3の利益の情報をサービスプロバイダ3に送信する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2の利益の情報をコンテンツプロバイダ2に送信する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、価格情報及び取扱方針の正当性を監査する。

図27は、EMDサービスセンタ1の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。経歴データ管理部15は、ユーザのコンテンツの使用実績を示す課金情報を著作権管理部13及び利益分配部16に送信する。利益分配部16は、JASRACに対する請求金額及び支払金額を算出し、その情報を出納部20に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。著作権管理部13は、ユーザのコンテンツの使用実績をJASRACに送信する。



次に、供給された、暗号化されているコンテンツをメモリスティックに記憶させ、不正の防止を図りつつ、そのコンテンツを他の再生装置などで利用できるようにしたユーザホームネットワーク 5 の実施の形態の構成を図 28 に示す。図 10 の場合と同様の部分には、同一の番号を付してあり、その説明は適宜省略する。なお、図 28 において、I C カードインターフェース 64 及び I C カード 55 の図示を省略する。

レシーバ 51 に装着され、コンテンツを記憶するメモリスティック 111 は、コンテンツ等の記憶等を制御する制御ブロック 121 及び実際にコンテンツ等を記憶する情報記憶ブロック 122 からなる。制御ブロック 121 は、シングルチップの暗号処理専用 I C で構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧又は周波数の幅が狭いなど、外部から不正にデータが読み出せない耐タンパー性を有する。

制御ブロック 121 は、通信部 121、メモリコントローラ 132、相互認証部 133、暗号化部 134、記憶部 135、復号部 136、乱数生成部 137 及びデータ検査部 138 からなる。通信部 131 は、レシーバ 51 から暗号化されたコンテンツ又は暗号化されたコンテンツ鍵 K c o 等を受信し、また、レシーバ 51 に暗号化されたコンテンツ又は暗号化されたコンテンツ鍵 K c o などを送信する。メモリコントローラ 132 は、通信部 131 が受信した暗号化されたコンテンツ又はコンテンツ鍵 K c o 等を、情報記憶ブロック 122 に書き込み、また、情報記憶ブロック 122 に書き込まれたコンテンツ等を読み出し、通信部 131 等に供給する。相互認証

部 1 3 3 は、レシーバ 5 1 の相互認証モジュール 7 1 と、相互認証処理により、相互認証し、相互認証後、レシーバ 5 1 との通信で、所定の期間利用される一時鍵  $K_{temp}$  を生成する。

暗号化部 1 3 4 は、一旦、復号部 1 3 6 が復号したコンテンツ鍵  $K_c o$  を、保存用鍵  $K_{save}$  で暗号化し、メモリコントローラ 1 3 2 に供給する。復号部 1 3 6 は、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_c o$  又は保存用鍵  $K_{save}$  で暗号化されたコンテンツ鍵  $K_c o$  などを復号し、暗号化部 1 3 4 又は通信部 1 3 1 に供給する。記憶部 1 3 5 は、そのメモリスティック 1 1 1 に固有の（メモリスティック 1 1 1 毎に、異なる）値を有する保存用鍵  $K_{save}$  及び検査用鍵  $K_{ch}$  などを記憶し、暗号化部 1 3 4 又は復号部 1 3 6 に供給する。記憶部 1 3 5 の記憶の態様については、図 3 4 及び図 3 6 で詳細に説明する。

乱数生成部 1 3 7 は、後述する情報記憶ブロック 1 2 2 に記憶されている平文（暗号化されていない）のコンテンツを、メモリスティック 1 1 1 内部で暗号化するときに必要な鍵である、所定の桁数の乱数を生成する。データ検査部 1 3 8 は、記憶部 1 3 5 に記憶されている所定の検査値（検査用のデータ）と後述する鍵データ 1 4 3 に記憶されている所定のデータのハッシュ値とを比較することにより、情報記憶ブロック 1 2 2 に記憶されている記憶されているコンテンツ鍵  $K_c o$  及び使用許諾情報などが改竄されていないか否かを検査する。データ検査部 1 3 8 は、また、情報記憶ブロック 1 2 2 に記憶されているコンテンツの移動又は情報記憶ブロック 1 2 2 へのコンテンツの書き込みのとき、所定の検査値を生成し、記憶部 1 3 5 に記憶させる。

情報記憶ブロック 122 は、EEPROM(Electrically Erasable Programmable Read Only Memory)、フラッシュメモリ、強誘電体メモリなどの電氣的に記憶内容を書換えできる、汎用の不揮発性メモリで構成され、データ検索用テーブル 141、識別情報 142、鍵データ 143、暗号化データ 144 及び非暗号化データ 145 が記憶される。データ検索用テーブル 141 には、鍵データ 143、暗号化データ 144 及び非暗号化データ 145 として記憶されている情報の内容とその記憶位置を表すデータが記憶されている。識別情報 142 には、記憶されている情報の内容が、暗号化されているか否かを示すデータが記憶される。鍵データ 143 としては、暗号化データ 144 に記憶されているコンテンツ毎に、コンテンツ鍵 K<sub>co</sub>、コンテンツ ID 及び使用許諾情報が記憶されている。鍵データ 143 の記憶の態様については、図 33 及び図 35 で詳細に説明する。暗号化データ 144 としては、暗号化されたコンテンツが記憶されている。非暗号化データ 145 としては、暗号化されていないコンテンツ及びその使用許諾情報等が記憶される。

図 28 のレシーバ 51 は、図 10 のレシーバ 51 に、メモリスティックインターフェース 112 及び外部記憶部 113 が追加されている構成を有する。メモリスティックインターフェース 112 は、SAM 62 からの信号を所定の形式に変更し、レシーバ 51 に装着されたメモリスティック 111 に出力し、また、メモリスティック 111 からの信号を所定の形式に変更し、SAM 62 に出力する。外部記憶部 113 は、汎用の不揮発性メモリで構成され、SAM 62 から供給されたコンテンツ鍵 K<sub>co</sub>などを記憶し、記憶しているコンテンツ鍵 K<sub>co</sub>などを SAM 62 に出力するようになされている。

る。外部記憶部 1 1 3 の記憶の態様については、図 2 9 及び図 3 1 で詳細に説明する。

さらに、図 2 8 の S A M 6 2 は、図 1 0 の S A M 6 2 データ検査モジュール 1 1 4 を有する。データ検査モジュール 1 1 4 は、記憶モジュール 7 3 に記憶されている所定の検査データと外部記憶部 1 1 3 が記憶する所定のデータのハッシュ値を比較することにより、外部記憶部 1 1 3 に記憶されている記憶されているコンテンツ鍵 K c o 及び使用許諾情報などが改竄されていないか否かを検査する。データ検査モジュール 1 1 4 は、また、H D D 5 2 に記憶されているコンテンツの移動又は H D D 5 2 へのコンテンツの書き込みのとき、所定の検査値を生成し、記憶モジュール 7 3 に記憶させる。

外部記憶部 1 1 3 の記憶の態様について、図 2 9 を参照して説明する。外部記憶部 1 1 3 の記憶領域は、所定の数の鍵データブロックに分割されている（図 2 9 では、5 つの鍵データブロックに分割されている）。それぞれの鍵データブロックは、例えば、2 組のコンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報を記憶できる。鍵データブロックに記憶されている 1 組のコンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報は、コンテンツ I D で特定される H D D 5 2 に記憶されているコンテンツに対応している。鍵データブロック 4 の前半部分に記憶されていたコンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報に対応するコンテンツが、H D D 5 2 から、メモリスティック 1 1 1 に移動したとき、鍵データブロック 4 の前半部分に記憶されていたコンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報は、消去され、図 2 9 に示すように、鍵データブロック 4 の前半部分にコンテンツ鍵 K c o 等が記憶されていない部

分が生じる。同様の操作で、図29の鍵データブロック3の後半部分もコンテンツ鍵K c o等が記憶されていない。

図30は、ユーザホームネットワーク5が、図28に示す構成を有するときの、記憶モジュール73の記憶の態様を説明する図である。図30の記憶モジュール73は、ユーザの秘密鍵K s u、課金情報、保存用鍵K s a v e及び配送用鍵K dに加えて、図29で説明した、外部記憶部113の鍵データブロックに対応する検査値を記憶する。例えば、記憶モジュール73の検査値1は、データ検査モジュール114が、外部記憶部113の鍵データブロック1のデータ（すなわち、コンテンツ鍵K c o 1、コンテンツI D 1、使用許諾情報1、コンテンツ鍵K c o 2、コンテンツI D 2及び使用許諾情報2）にハッシュ関数を適用して得られた値であり、同様に、検査値2は、データ検査モジュール114が、鍵データブロック2のデータにハッシュ関数を適用して得られた値である。検査値3、検査値4及び検査値5は、同様に、鍵データブロック3、鍵データブロック4及び鍵データブロック5にそれぞれ対応する。

すなわち、例えば、鍵データブロック3にハッシュ関数を適用して得られたハッシュ値と検査値3が一致すれば、鍵データブロック3に記憶されているコンテンツ鍵K c o 5、コンテンツI D 5及び使用許諾情報5は、改竄されていないことがわかる。一方、鍵データブロック3にハッシュ関数を適用して得られたハッシュ値と検査値3が一致しなければ、鍵データブロック3に記憶されているコンテンツ鍵K c o 5、コンテンツI D 5及び使用許諾情報5のいずれかが、改竄されていると判定できる。

検査値は、耐タンパー性のあるS A M 6 2の記憶モジュール73

に記憶され、外部から不正に読み出すことが困難であるので、改竄が防止され、したがって、図 28 に示すレシーバ 51 に記憶されたコンテンツ鍵 K c o 及び H D D 52 に記憶されたコンテンツは、不正に対して極めて耐性が高い。

図 31 は、外部記憶部 113 の他の記憶の態様を説明する図である。図 31 に示す場合、外部記憶部 113 は、コンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報の組に加えて、鍵データブロックに対応した検査値も記憶する。図 31 における、例えば、外部記憶部 113 の検査値 1 は、データ検査モジュール 114 が、外部記憶部 113 の鍵データブロック 1 のデータ（すなわち、コンテンツ鍵 K c o 1、コンテンツ I D 1、使用許諾情報 1、コンテンツ鍵 K c o 2、コンテンツ I D 2 及び使用許諾情報 2）にハッシュ関数を適用して得られた値を、さらに、記憶モジュール 73 に記憶する、レシーバ 51 特有の値を有する検査用鍵 K c h で暗号化した値である。検査値 2、検査値 3、検査値 4 及び検査値 5 は、同様に、鍵データブロック 2、鍵データブロック 3、鍵データブロック 4 及び鍵データブロック 5 にそれぞれ対応する。

図 32 は、ユーザホームネットワーク 5 が、図 28 に示す構成を有し、外部記憶部 113 が、図 31 に示す記憶の態様を有するときの、記憶モジュール 73 の記憶の態様を説明する図である。図 32 の記憶モジュール 73 は、レシーバ 51（ユーザ）の秘密鍵 K s u、課金情報、保存用鍵 K s a v e 及び配送用鍵 K d に加えて、検査用鍵 K c h が記憶されている。

すなわち、例えば、外部記憶部 113 の鍵データブロック 3 にハッシュ関数を適用して得られたハッシュ値と、外部記憶部 113 の

検査値 3 を検査用鍵 K c h で復号した値が一致すれば、外部記憶部 1 1 3 の鍵データブロック 3 に記憶されているコンテンツ鍵 K c o 5、コンテンツ I D 5 及び使用許諾情報 5 は、改竄されていないことがわかる。一方、外部記憶部 1 1 3 の鍵データブロック 3 にハッシュ関数を適用して得られたハッシュ値と、外部記憶部 1 1 3 の検査値 3 を検査用鍵 K c h で復号した値が一致しなければ、外部記憶部 1 1 3 の鍵データブロック 3 に記憶されているコンテンツ鍵 K c o 5、コンテンツ I D 5 及び使用許諾情報 5 のいずれかが、改竄されていると判定できる。

図 2 9 及び図 3 0 に示す場合に比較し、図 3 1 に示す外部記憶部 1 1 3 及び図 3 2 に示す記憶モジュール 7 3 は、検査値が耐タンパー性を有するメモリに較べ低価格な汎用メモリに記憶されるので、大量のコンテンツに対応する検査値を記憶できるレシーバ 5 1 が、安価に実現できる。

次に、鍵データ 1 4 3 の記憶の態様について、図 3 3 を参照して説明する。鍵データ 1 4 3 の記憶領域は、所定の数の鍵データブロックに分割されている（図 3 3 では、4 つの鍵データブロックに分割されている）。それぞれの鍵データブロックは、例えば、2 組のコンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報を記憶できる。鍵データブロックに記憶されている 1 組のコンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報は、コンテンツ I D で特定される暗号化データ 1 4 4 に記憶されているコンテンツに対応している。鍵データブロック 3 の後半部分に記憶されていたコンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報に対応するコンテンツが、メモリスティック 1 1 1 から、H D D 5 2 に移動したとき、鍵データ

ブロック 4 の後半部分に記憶されていたコンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報は、消去され、図 3 3 に示すように、鍵データブロック 4 の後半部分にコンテンツ鍵 K c o 等が記憶されていない部分が生じる。

図 3 4 は、ユーザホームネットワーク 5 が、図 2 8 に示す構成を有するときの、記憶部 1 3 5 の記憶の態様を説明する図である。記憶部 1 3 5 は、ユーザの秘密鍵 K s u、保存用鍵 K s a v e、及び、図 3 3 で説明した鍵データ 1 4 3 の鍵データブロックに対応する検査値と必要に応じて課金情報を記憶する。例えば、記憶部 1 3 5 の検査値 1 は、データ検査部 1 3 8 が、鍵データ 1 4 3 の鍵データブロック 1 のデータ（すなわち、コンテンツ鍵 K c o 1、コンテンツ I D 1、使用許諾情報 1、コンテンツ鍵 K c o 2、コンテンツ I D 2 及び使用許諾情報 2）にハッシュ関数を適用して得られた値であり、同様に、検査値 2 は、データ検査部 1 3 8 が、鍵データブロック 2 のデータにハッシュ関数を適用して得られた値である。検査値 3 及び検査値 4 は、同様に、鍵データブロック 3 及び鍵データブロック 4 にそれぞれ対応する。

すなわち、例えば、鍵データ 1 4 3 の鍵データブロック 3 にハッシュ関数を適用して得られたハッシュ値と記憶部 1 3 5 の検査値 3 が一致すれば、鍵データ 1 4 3 の鍵データブロック 3 に記憶されているコンテンツ鍵 K c o 5、コンテンツ I D 5 及び使用許諾情報 5 は、改竄されていないことがわかる。一方、鍵データブロック 3 にハッシュ関数を適用して得られたハッシュ値と検査値 3 が一致しなければ、鍵データブロック 3 に記憶されているコンテンツ鍵 K c o 5、コンテンツ I D 5 及び使用許諾情報 5 のいずれかが、改竄され



ていると判定できる。

レシーバ51のときと同様に、メモリスティック111の検査値は、耐タンパー性のある制御ブロック121の記憶部135に記憶され、外部から不正に読み出すことが困難であるので、改竄が防止され、したがって、図28に示すメモリスティック111に記憶されたコンテンツ鍵Kco及びコンテンツは、不正に対して極めて耐性が高い。

図35は、鍵データ143の他の記憶の態様を説明する図である。図35に示す場合、鍵データ143は、コンテンツ鍵Kco、コンテンツID及び使用許諾情報の組に加えて、鍵データブロックに対応した検査値も記憶する。図35における、例えば、鍵データ143の検査値1は、データ検査部138が、鍵データ143の鍵データブロック1のデータ（すなわち、コンテンツ鍵Kco1、コンテンツID1、使用許諾情報1、コンテンツ鍵Kco2、コンテンツID2及び使用許諾情報2）にハッシュ関数を適用して得られた値を、さらに、記憶部135に記憶する、メモリスティック111特有の値を有する検査用鍵Kch（したがって、レシーバ51の記憶モジュール73が記憶する検査用鍵Kchとは、その値が異なる）で暗号化した値である。検査値2、検査値3及び検査値4は、同様に、鍵データブロック2、鍵データブロック3及び鍵データブロック4にそれぞれ対応する。

図36は、ユーザホームネットワーク5が、図28に示す構成を有し、メモリスティック111の鍵データ143が、図35に示す記憶の態様を有するときの、記憶部135の記憶の態様を説明する図である。図36の記憶部135は、メモリスティック111の秘

密鍵  $K_{su2}$  及び保存用鍵  $K_{save}$  に加えて、検査用鍵  $K_{ch}$  が記憶されている。

すなわち、例えば、鍵データ 143 の鍵データブロック 3 にハッシュ関数を適用して得られたハッシュ値と、鍵データ 143 の検査値 3 を検査用鍵  $K_{ch}$  で復号した値が一致すれば、鍵データ 143 の鍵データブロック 3 に記憶されているコンテンツ鍵  $K_{co5}$ 、コンテンツ ID 5 及び使用許諾情報 5 は、改竄されていないことがわかる。一方、鍵データ 143 の鍵データブロック 3 にハッシュ関数を適用して得られたハッシュ値と鍵データ 143 の検査値 3 を検査用鍵  $K_{ch}$  で復号した値が一致しなければ、鍵データ 143 の鍵データブロック 3 に記憶されているコンテンツ鍵  $K_{co5}$ 、コンテンツ ID 5 及び使用許諾情報 5 のいずれかが、改竄されていると判定できる。

図 35 に示す鍵データ 143 及び図 36 に示す記憶部 135 は、検査値が耐タンパー性を有するメモリに較べ低価格な汎用メモリに記憶されるので、大量のコンテンツに対応する検査値を記憶できるメモリスティック 111 が、安価に実現できる。

次に、EMD システムの処理について説明する。図 37 は、このシステムのコンテンツの配布及び再生の処理を説明するフローチャートである。ステップ S11 において、EMD サービスセンタ 1 のコンテンツプロバイダ管理部 12 は、コンテンツプロバイダ 2 に配送用鍵  $K_d$  を送信し、コンテンツプロバイダ 2 がこれを受信する。その処理の詳細は、図 39 のフローチャートを参照して後述する。ステップ S12 において、ユーザは、ユーザホームネットワーク 5 の機器（例えば、図 10 のレシーバ 51）を操作し、ユーザホーム

ネットワーク 5 の機器を EMD サービスセンタ 1 のユーザ管理部 18 に登録する。この登録処理の詳細は、図 4 3 のフローチャートを参照して後述する。ステップ S 1 3 において、EMD サービスセンタ 1 のユーザ管理部 18 は、ユーザホームネットワーク 5 と、図 4 0 乃至図 4 2 に示したように相互認証した後、ユーザホームネットワーク 5 の機器に、配送用鍵 K d を送信する。ユーザホームネットワーク 5 はこの鍵を受信する。この処理の詳細は、図 5 2 のフローチャートを参照して説明する。

ステップ S 1 4 において、コンテンツプロバイダ 2 のセキュアコンテンツ作成部 3 8 は、サービスプロバイダ 3 にコンテンツプロバイダセキュアコンテンツを送信する。この送信処理の詳細は、図 5 4 のフローチャートを参照して後述する。ステップ S 1 5 において、サービスプロバイダ 3 のセキュアコンテンツ作成部 4 4 は、ユーザホームネットワーク 5 からの要求に応じて、ネットワーク 4 を介して、ユーザホームネットワーク 5 にサービスプロバイダセキュアコンテンツを送信する。この送信処理の詳細は、図 5 5 のフローチャートを参照して後述する。ステップ S 1 6 において、ユーザホームネットワーク 5 の課金モジュール 7 2 は、課金処理を実行する。課金処理の詳細は、図 5 6 のフローチャートを参照して後述する。ステップ S 1 7 において、ユーザは、ユーザホームネットワーク 5 の機器でコンテンツを再生する。再生処理の詳細は、図 7 8 のフローチャートを参照して後述する。

一方、コンテンツプロバイダ 2 が、取扱方針を暗号化して送信する場合の処理は、図 3 8 のフローチャートで示すようになる。ステップ S 2 1 において、EMD サービスセンタ 1 のコンテンツプロバ

イダ管理部 1 2 は、コンテンツプロバイダ 2 に配送用鍵 K d を送信する。ステップ S 2 2 において、EMD サービスセンタ 1 のサービスプロバイダ管理部 1 1 は、サービスプロバイダ 3 に配送用鍵 K d を送信する。それ以降のステップ S 2 3 乃至ステップ S 2 8 の処理は、図 3 7 のステップ S 1 2 乃至ステップ S 1 7 の処理と同様の処理であり、その説明は省略する。

図 3 9 は、図 3 7 のステップ S 1 1 及び図 3 8 のステップ S 2 1 に対応する、EMD サービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信し、コンテンツプロバイダ 2 がこれを受信する処理の詳細を説明するフローチャートである。ステップ S 3 1 において、EMD サービスセンタ 1 の相互認証部 1 7 は、コンテンツプロバイダ 2 の相互認証部 3 9 と相互認証する。この相互認証処理の詳細は、図 4 0 を参照して後述する。相互認証処理により、コンテンツプロバイダ 2 が、正当なプロバイダであることが確認されたとき、ステップ S 3 2 において、コンテンツプロバイダ 2 の暗号化部 3 4 及び暗号化部 3 6 は、EMD サービスセンタ 1 のコンテンツプロバイダ管理部 1 2 から送信された配送用鍵 K d を受信する。ステップ S 3 3 において、コンテンツプロバイダ 2 の暗号化部 3 4 は、受信した配送用鍵 K d を記憶する。

このように、コンテンツプロバイダ 2 は、EMD サービスセンタ 1 から配送用鍵 K d を受け取る。同様に、図 3 8 に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ 2 以外に、サービスプロバイダ 3 も、図 3 9 と同様の処理で、EMD サービスセンタ 1 から配送用鍵 K d を受け取る。

次に、図 3 9 のステップ S 3 1 における、いわゆるなりすましが

ないことを確認する相互認証の処理について、1つの共通鍵を用いる（図40）、2つの共通鍵を用いる（図41）及び公開鍵暗号を用いる（図42）を例として説明する。

図40は、1つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS41において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する（乱数生成部35が生成するようにしてもよい）。ステップS42において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数R1を、予め記憶している共通鍵Kcで暗号化する（暗号化部36で暗号化するようにしてもよい）。ステップS43において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R1をEMDサービスセンタ1の相互認証部17に送信する。

ステップS44において、EMDサービスセンタ1の相互認証部17は、受信した乱数R1を予め記憶している共通鍵Kcで復号する。ステップS45において、EMDサービスセンタ1の相互認証部17は、32ビットの乱数R2を生成する。ステップS46において、EMDサービスセンタ1の相互認証部17は、復号した64ビットの乱数R1の下位32ビットを乱数R2で入れ替え、接続R1H || R2を生成する。なお、ここでRiHは、Riの上位ビットを表し、A || Bは、AとBの接続（nビットのAの下位に、mビットのBを結合して、（n+m）ビットとしたもの）を表す。ステップS47において、EMDサービスセンタ1の相互認証部17は、DESを用いてR1H || R2を共通鍵Kcで暗号化する。ステップ

S 4 8において、E M Dサービスセンタ 1の相互認証部 1 7は、暗号化した $R 1 H \parallel R 2$ をコンテンツプロバイダ 2に送信する。

ステップS 4 9において、コンテンツプロバイダ 2の相互認証部 3 9は、受信した $R 1 H \parallel R 2$ を共通鍵 $K c$ で復号する。ステップS 5 0において、コンテンツプロバイダ 2の相互認証部 3 9は、復号した $R 1 H \parallel R 2$ の上位3 2ビット $R 1 H$ を調べ、ステップS 4 1で生成した、乱数 $R 1$ の上位3 2ビット $R 1 H$ と一致すれば、E M Dサービスセンタ 1が正当なセンタであることを認証する。生成した乱数 $R 1 H$ と、受信した $R 1 H$ が一致しないとき、処理は終了される。両者が一致するとき、ステップS 5 1において、コンテンツプロバイダ 2の相互認証部 3 9は、3 2ビットの乱数 $R 3$ を生成する。ステップS 5 2において、コンテンツプロバイダ 2の相互認証部 3 9は、受信し、復号した3 2ビットの乱数 $R 2$ を上位に設定し、生成した乱数 $R 3$ をその下位に設定し、接続 $R 2 \parallel R 3$ とする。ステップS 5 3において、コンテンツプロバイダ 2の相互認証部 3 9は、D E Sを用いて接続 $R 2 \parallel R 3$ を共通鍵 $K c$ で暗号化する。ステップS 5 4において、コンテンツプロバイダ 2の相互認証部 3 9は、暗号化された接続 $R 2 \parallel R 3$ をE M Dサービスセンタ 1の相互認証部 1 7に送信する。

ステップS 5 5において、E M Dサービスセンタ 1の相互認証部 1 7は、受信した接続 $R 2 \parallel R 3$ を共通鍵 $K c$ で復号する。ステップS 5 6において、E M Dサービスセンタ 1の相互認証部 1 7は、復号した接続 $R 2 \parallel R 3$ の上位3 2ビットを調べ、乱数 $R 2$ と一致すれば、コンテンツプロバイダ 2を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

図41は、2つの共通鍵 $K_c1$ 、 $K_c2$ で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS61において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数 $R_1$ を生成する。ステップS62において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数 $R_1$ を予め記憶している共通鍵 $K_c1$ で暗号化する。ステップS63において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数 $R_1$ をEMDサービスセンタ1に送信する。

ステップS64において、EMDサービスセンタ1の相互認証部17は、受信した乱数 $R_1$ を予め記憶している共通鍵 $K_c1$ で復号する。ステップS65において、EMDサービスセンタ1の相互認証部17は、乱数 $R_1$ を予め記憶している共通鍵 $K_c2$ で暗号化する。ステップS66において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数 $R_2$ を生成する。ステップS67において、EMDサービスセンタ1の相互認証部17は、乱数 $R_2$ を共通鍵 $K_c2$ で暗号化する。ステップS68において、EMDサービスセンタ1の相互認証部17は、暗号化された乱数 $R_1$ 及び乱数 $R_2$ をコンテンツプロバイダ2の相互認証部39に送信する。

ステップS69において、コンテンツプロバイダ2の相互認証部39は、受信した乱数 $R_1$ 及び乱数 $R_2$ を予め記憶している共通鍵 $K_c2$ で復号する。ステップS70において、コンテンツプロバイダ2の相互認証部39は、復号した乱数 $R_1$ を調べ、ステップS61で生成した乱数 $R_1$ （暗号化する前の乱数 $R_1$ ）と一致すれば、

EMDサービスセンタ 1 を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップ S 7 1 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、復号して得た乱数 R 2 を共通鍵 K c 1 で暗号化する。ステップ S 7 2 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、暗号化された乱数 R 2 を EMD サービスセンタ 1 に送信する。

ステップ S 7 3 において、EMD サービスセンタ 1 の相互認証部 1 7 は、受信した乱数 R 2 を共通鍵 K c 1 で復号する。ステップ S 7 4 において、EMD サービスセンタ 1 の相互認証部 1 7 は、復号した乱数 R 2 が、ステップ S 6 6 で生成した乱数 R 2（暗号化する前の乱数 R 2）と一致すれば、コンテンツプロバイダ 2 を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

図 4 2 は、公開鍵暗号である、1 6 0 ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ 2 の相互認証部 3 9 と EMD サービスセンタ 1 の相互認証部 1 7 との相互認証の動作を説明するフローチャートである。ステップ S 8 1 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、6 4 ビットの乱数 R 1 を生成する。ステップ S 8 2 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、自分自身の公開鍵 K p c p を含む証明書（認証局から予め取得しておいたもの）と、乱数 R 1 を EMD サービスセンタ 1 の相互認証部 1 7 に送信する。

ステップ S 8 3 において、EMD サービスセンタ 1 の相互認証部 1 7 は、受信した証明書の署名（認証局の秘密鍵 K s c a で暗号化されている）を、予め取得しておいた認証局の公開鍵 K p c a で復



号し、コンテンツプロバイダ 2 の公開鍵  $K_{pcp}$  とコンテンツプロバイダ 2 の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ 2 の公開鍵  $K_{pcp}$  及びコンテンツプロバイダ 2 の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵  $K_{pcp}$  及びコンテンツプロバイダ 2 の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ 2 の公開鍵  $K_{pcp}$  及びコンテンツプロバイダ 2 の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵  $K_{pcp}$  が改竄されたものでない適正なものであることが認証される。署名を復号できなかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

適正な認証結果が得られたとき、ステップ S 8 4 において、EMD サービスセンタ 1 の相互認証部 1 7 は、64 ビットの乱数  $R_2$  を生成する。ステップ S 8 5 において、EMD サービスセンタ 1 の相互認証部 1 7 は、乱数  $R_1$  及び乱数  $R_2$  の接続  $R_1 \parallel R_2$  を生成する。ステップ S 8 6 において、EMD サービスセンタ 1 の相互認証部 1 7 は、接続  $R_1 \parallel R_2$  を自分自身の秘密鍵  $K_{sesc}$  で暗号化する。ステップ S 8 7 において、EMD サービスセンタ 1 の相互認証部 1 7 は、接続  $R_1 \parallel R_2$  を、ステップ S 8 3 で取得したコンテンツプロバイダ 2 の公開鍵  $K_{pcp}$  で暗号化する。ステップ S 8 8 において、EMD サービスセンタ 1 の相互認証部 1 7 は、秘密鍵  $K_{sesc}$  で暗号化された接続  $R_1 \parallel R_2$ 、公開鍵  $K_{pcp}$  で暗号化された接続  $R_1 \parallel R_2$  及び自分自身の公開鍵  $K_{pesc}$  を含む証明

書（認証局から予め取得しておいたもの）をコンテンツプロバイダ 2 の相互認証部 39 に送信する。

ステップ S 8 9 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信した証明書の署名を予め取得しておいた認証局の公開鍵  $K_{pca}$  で復号し、正しければ証明書から公開鍵  $K_{pesc}$  を取り出す。この場合の処理は、ステップ S 8 3 における場合と同様であるので、その説明は省略する。ステップ S 9 0 において、コンテンツプロバイダ 2 の相互認証部 39 は、EMD サービスセンタ 1 の秘密鍵  $K_{sesc}$  で暗号化されている接続  $R_1 \parallel R_2$  を、ステップ S 8 9 で取得した公開鍵  $K_{pesc}$  で復号する。ステップ S 9 1 において、コンテンツプロバイダ 2 の相互認証部 39 は、自分自身の公開鍵  $K_{pcp}$  で暗号化されている接続  $R_1 \parallel R_2$  を、自分自身の秘密鍵  $K_{scp}$  で復号する。ステップ S 9 2 において、コンテンツプロバイダ 2 の相互認証部 39 は、ステップ S 9 0 で復号された接続  $R_1 \parallel R_2$  と、ステップ S 9 1 で復号された接続  $R_1 \parallel R_2$  を比較し、一致すれば EMD サービスセンタ 1 を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

適正な認証結果が得られたとき、ステップ S 9 3 において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数  $R_3$  を生成する。ステップ S 9 4 において、コンテンツプロバイダ 2 の相互認証部 39 は、ステップ S 9 0 で取得した乱数  $R_2$  及び生成した乱数  $R_3$  の接続  $R_2 \parallel R_3$  を生成する。ステップ S 9 5 において、コンテンツプロバイダ 2 の相互認証部 39 は、接続  $R_2 \parallel R_3$  を、ステップ S 8 9 で取得した公開鍵  $K_{pesc}$  で暗号化する。ステップ S 9 6 において、コンテンツプロバイダ 2 の相互認証部 39 は、

暗号化した接続  $R2 \parallel R3$  を EMD サービスセンタ 1 の相互認証部 17 に送信する。

ステップ S 97 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化された接続  $R2 \parallel R3$  を自分自身の秘密鍵  $K_{sec}$  で復号する。ステップ S 98 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した乱数  $R2$  が、ステップ S 84 で生成した乱数  $R2$ （暗号化する前の乱数  $R2$ ）と一致すれば、コンテンツプロバイダ 2 を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

以上のように、EMD サービスセンタ 1 の相互認証部 17 とコンテンツプロバイダ 2 の相互認証部 39 は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵  $K_{temp}$  として利用される。

図 43 は、図 37 のステップ S 12 及び図 38 のステップ S 23 に対応する、レシーバ 51 が EMD サービスセンタ 1 のユーザ管理部 18 に登録する処理を説明するフローチャートである。ステップ S 101 において、レシーバ 51 の SAM 62 は、IC カードインターフェース 64 の出力から、レシーバ 51 にバックアップ用の IC カード 55 が装着されているか否かを判定し、バックアップ用の IC カード 55 が装着されていると判定された場合（例えば、レシーバ 51 が新たなレシーバ 51 に変更され、元のレシーバ 51 のデータを、新たなレシーバ 51 に引き継ぐために、元のレシーバ 51 のデータをバックアップ用の IC カード 55 にバックアップさせている場合）、ステップ S 102 に進み、IC カード 55 に記憶されているバックアップデータの読み込み処理を実行する。この処理の

詳細は、図 4 8 のフローチャートを参照して後述する。勿論、この読み込み処理が実行されるためには、その前に、I C カード 5 5 に、バックアップデータを記憶させる必要があるが、その処理は、図 4 6 を参照して後述する。

ステップ S 1 0 1 において、バックアップ用の I C カード 5 5 が装着されていないと判定された場合、ステップ S 1 0 3 に進む。ステップ S 1 0 3 において、S A M 6 2 の相互認証モジュール 7 1 は、E M D サービスセンタ 1 の相互認証部 1 7 と相互認証し、S A M 6 2 は、証明書を E M D サービスセンタ 1 のユーザ管理部 1 8 に送信する。この認証処理は、図 4 0 乃至図 4 2 を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S 1 0 3 で、S A M 6 2 が E M D サービスセンタ 1 のユーザ管理部 1 8 に送信する署名書は、図 4 4 に示すデータを含む。S A M 6 2 が送信する証明書は、図 1 4 に示すコンテンツプロバイダ 2 の証明書とほぼ同様の構成を有するが、さらに、他の S A M に従属するか否かを示すデータを含んでいる。ステップ S 1 0 4 において、S A M 6 2 は、通信部 6 1 を介して、一時鍵 K t e m p で暗号化した、ユーザの銀行等の決済機関の情報等を E M D サービスセンタ 1 のユーザ管理部 1 8 に送信する。

ステップ S 1 0 5 において、E M D サービスセンタ 1 のユーザ管理部 1 8 は、受信した S A M 6 2 の I D を基に、図 7 に示したユーザ登録データベースを検索する。ステップ S 1 0 6 において、E M D サービスセンタ 1 のユーザ管理部 1 8 は、受信した I D を有する S A M 6 2 の登録が可能であるか否かを判定し、受信した I D を有する S A M 6 2 の登録が可能であると判定された場合、ステップ S

107に進み、受信したIDを有するSAM62が、新規登録であるか否かを判定する。ステップS107において、受信したIDを有するSAM62が、新規登録ではないと判定された場合、手続は、ステップS108に進む。

ステップS108において、EMDサービスセンタ1のユーザ管理部18は、更新登録を実行し、受信したIDを基にユーザ登録データベースを検索し、登録リストを作成する。この登録リストは、例えば、図45に示す構造を有し、機器のSAMのIDに対応して、EMDサービスセンタ1のユーザ管理部18が登録を拒絶したか否かを示す登録拒絶フラグ、従属する機器である場合のコンテンツ鍵Kcoの利用条件を示すステータスフラグ、従属する機器であるか否かを示すコンディションフラグ並びに登録拒絶フラグ、ステータスフラグ及びコンディションフラグにハッシュ関数を適用して生成したハッシュ値をEMDサービスセンタ1の秘密鍵Ksecで暗号化した署名から構成される。

機器のSAMのIDは、機器の固有の64ビットからなるIDを示す（図45では、16進数で示す）。登録拒絶フラグの”1”は、EMDサービスセンタ1のユーザ管理部18が対応するIDを有する機器を登録したことを示し、登録拒絶フラグの”0”は、MDサービスセンタ1のユーザ管理部18が対応するIDを有する機器の登録を拒絶したことを示す。

ステータスフラグのMSB(Most Significant Bit)の”1”は、対応するIDを有する子の機器（例えばレコード53）が従属した親の機器（例えばレシーバ51）からコンテンツ鍵Kcoをもらえることを示し、ステータスフラグのMSBの”0”は、対応するI

Dを有する子の機器が従属した親の機器からコンテンツ鍵K c oをもらえないことを示している。ステータスフラグの上位から2ビット目の”1”は、対応するIDを有する子の機器が従属した親の機器から、親の機器の保存用鍵K s a v eで暗号化されたコンテンツ鍵K c oをもらえることを示す。ステータスフラグの上位から3ビット目の”1”は、対応するIDを有する子の機器が従属した親の機器から、配送用鍵K dで暗号化されたコンテンツ鍵K c oをもらえることを示す。ステータスフラグのLSB(Least Significant Bit)の”1”は、従属した親の機器が配送用鍵K dで暗号化したコンテンツ鍵K c oを購入し、対応するIDを有する子の機器に、一時鍵K t e m pで暗号化してコンテンツ鍵K c oを渡すことを示す。

コンディションフラグの”0”は、対応するIDを有する機器がEMDサービスセンタ1のユーザ管理部18と直接通信ができる(すなわち、例えばレシーバ51のような親の機器である)ことを示し、コンディションフラグの”1”は、対応するIDを有する機器がEMDサービスセンタ1のユーザ管理部18と直接通信ができない(すなわち、例えばレコーダ53のような子の機器である)ことを示す。コンディションフラグが”0”のとき、ステータスフラグは常に”0000”に設定される。

ステップS109において、EMDサービスセンタ1のユーザ管理部18は、相互認証部17から供給された一時鍵K t e m pで暗号化した、鍵サーバ14から供給された配送用鍵K dをレシーバ51のSAM62に送信する。ステップS110において、レシーバ51のSAM62は、受信した配送用鍵K dを一時鍵K t e m pで復号し、記憶モジュール73に記憶させる。

ステップS 1 1 1において、E M Dサービスセンタ 1のユーザ管理部 1 8は、一時鍵K t e m pで暗号化した登録リストをレシーバ 5 1のS A M 6 2に送信する。ステップS 1 1 2において、レシーバ 5 1のS A M 6 2は、受信した登録リストを一時鍵K t e m pで復号し、記憶モジュール 7 3に記憶させ、処理は終了する。

ステップS 1 0 7において、受信したI Dを有するS A M 6 2が、新規登録であると判定された場合、手続は、ステップS 1 1 4に進み、E M Dサービスセンタ 1のユーザ管理部 1 8は、新規登録を実行し、登録リストを作成し、ステップS 1 0 9に進む。

ステップS 1 0 6において、受信したI Dを有するS A M 6 2の登録が不可であると判定された場合、ステップS 1 1 3に進み、E M Dサービスセンタ 1のユーザ管理部 1 8は、登録拒絶の登録リストを作成し、ステップS 1 1 1に進む。

このように、レシーバ 5 1は、E M Dサービスセンタ 1に登録される。

次に、今まで使用していたレシーバ 5 1の記憶モジュール 7 3に記憶された配送用鍵K dなどの所定のデータをI Cカード 5 5に記憶させる処理の詳細を、図 4 6のフローチャートを参照して説明する。ステップS 1 2 1において、S A M 6 2の相互認証モジュール 7 1は、I Cカード 5 5の相互認証モジュール 8 0と相互認証する。この認証処理は、図 4 0乃至図 4 2を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 2 2において、S A M 6 2の乱数発生ユニット 9 2は、バックアップ鍵K i cとして用いられる乱数を生成する。ステップS 1 2 3において、S A M 6 2の暗号化ユニット 9 3は、記憶モジュール 7 3に記憶されてい

るSAMのID番号、保存用鍵K s a v e及びHDD 5 2のIDを、バックアップ鍵K i cを用いて暗号化する。ステップS 1 2 4において、SAM 6 2の暗号化ユニット9 3は、EMDサービスセンタ1の公開鍵K p e s cでバックアップ鍵K i cを暗号化する（SAM 6 2は、EMDサービスセンタ1との間の認証処理（図4 2のステップS 8 9）において、EMDサービスセンタ1の公開鍵K p e s cを取得している）。ステップS 1 2 5において、レシーバ5 1のSAM 6 2は、ICカードインターフェース6 4を介して、暗号化されたSAMのID番号、保存用鍵K s a v e及びHDD 5 2のID並びに暗号化されたバックアップ鍵K i cをICカード5 5に送信し、記憶モジュール8 1に記憶させる。

以上のように、SAM 6 2の記憶モジュール7 3に記憶されたSAMのID番号、保存用鍵K s a v e及びHDD 5 2のIDは、バックアップ鍵K i cを用いて暗号化され、EMDサービスセンタ1の公開鍵K p e s cを用いて暗号化されたバックアップ鍵K i cとともに、ICカード5 5の記憶モジュール8 1に記憶される。

今まで使用していたレシーバ5 1の記憶モジュール7 3に記憶された配送用鍵K dなどの所定のデータをICカード5 5に記憶させる他の処理の例の詳細を、図4 7のフローチャートを参照して説明する。ステップS 1 3 1において、SAM 6 2の相互認証モジュール7 1は、ICカード5 5の相互認証モジュール8 0と相互認証する。ステップS 1 3 2において、SAM 6 2の暗号化ユニット9 3は、記憶モジュール7 3に記憶されているSAMのID番号、保存用鍵K s a v e及びHDD 5 2のIDを、EMDサービスセンタ1の公開鍵K p e s cを用いて暗号化する。ステップS 1 3 3におい



て、レシーバ51のSAM62は、ICカードインターフェース64を介して、暗号化されたSAMのID番号、保存用鍵Ksave及びHDD52のIDをICカード55に送信し、記憶モジュール81に記憶させる。

図47に示す処理により、図46に示した場合より簡単な処理で、EMDサービスセンタ1の公開鍵Kpescを用いて暗号化されたSAMのID番号、保存用鍵Ksave及びHDD52のIDは、ICカード55の記憶モジュール81に記憶される。

このように、ICカード55にバックアップされたデータは、図43のステップS102の処理で、新しいレシーバ51に読み込まれる。図48は、図46に示す処理でバックアップされたデータ読み出す場合の処理を説明するフローチャートである。ステップS141において、新しいレシーバ51のSAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。この認証処理は、図40乃至図42を参照して説明した場合と同様であるので、ここでは説明を省略する。

ステップS142において、SAM62は、ICカードインターフェース64を介して、記憶モジュール81に記憶された、バックアップ鍵Kicで暗号化されている古いレシーバ51の記憶モジュール73のデータ（SAMのID番号、保存用鍵Ksave及びHDD52のIDを示すバックアップデータ）及びEMDサービスセンタ1の公開鍵Kpescで暗号化されているバックアップ鍵Kicを読み出す。ステップS143において、SAM62の相互認証モジュール71は、通信部61を介して、EMDサービスセンタ1の相互認証部17と相互認証する。この認証処理は、図40乃至図4

2を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 4 4において、SAM 6 2は、通信部6 1を介して、バックアップ鍵K i cで暗号化されている記憶モジュール7 3のデータ及びEMDサービスセンタ1の公開鍵K p e s cで暗号化されているバックアップ鍵K i cを、EMDサービスセンタ1のユーザ管理部1 8に送信する。

ステップS 1 4 5において、EMDサービスセンタ1のユーザ管理部1 8は、受信したバックアップ鍵K i cを自分自身の秘密鍵K s e s cで復号する。ステップS 1 4 6において、EMDサービスセンタ1のユーザ管理部1 8は、受信したバックアップデータを、バックアップ鍵K i cで復号する。ステップS 1 4 7において、EMDサービスセンタ1のユーザ管理部1 8は、復号したバックアップデータを、相互認証部1 7から供給された一時鍵K t e m pで、再度、暗号化する。ステップS 1 4 8において、EMDサービスセンタ1のユーザ管理部1 8は、一時鍵K t e m pで暗号化されたバックアップデータを、レシーバ5 1の通信部6 1に送信する。

ステップS 1 4 9において、レシーバ5 1の通信部6 1は、EMDサービスセンタ1のユーザ管理部1 8から受信したデータを、SAM 6 2に送信し、SAM 6 2は、そのデータを復号した後、記憶モジュール7 3に記憶させる。ステップS 1 6 0において、EMDサービスセンタ1のユーザ管理部1 8は、ICカード5 5にデータを記憶させた古い装置のSAM 6 2のIDに対応するユーザ登録データベース（図7）のデータを登録不可に設定し、処理を終了する。

このように、新しいレシーバ5 1は、ICカード5 5のバックアップデータを読み込む。

また、図43のステップS102は、図49に示すフローチャートで説明される処理でもよい。ステップS151乃至ステップS153は、図48のステップS141乃至ステップS143とそれぞれ同様であるので、その説明は省略する。ステップS154において、SAM62は、通信部61を介して、EMDサービスセンタ1の公開鍵K<sub>pub</sub>で暗号化されているバックアップ鍵K<sub>ic</sub>を、EMDサービスセンタ1のユーザ管理部18に送信する。

ステップS155において、EMDサービスセンタ1のユーザ管理部18は、受信したバックアップ鍵K<sub>ic</sub>を自分自身の秘密鍵K<sub>sec</sub>で復号する。ステップS156において、EMDサービスセンタ1のユーザ管理部18は、復号したバックアップ鍵K<sub>ic</sub>を、相互認証部17から供給された一時鍵K<sub>temp</sub>で、再度、暗号化する。ステップS157において、EMDサービスセンタ1のユーザ管理部18は、一時鍵K<sub>temp</sub>で暗号化されたバックアップ鍵K<sub>ic</sub>を、レシーバ51の通信部61に送信し、バックアップ鍵K<sub>ic</sub>の復号のサービスに対するユーザへの課金の処理をする。

ステップS158において、レシーバ51の通信部61は、EMDサービスセンタ1のユーザ管理部18から受信した一時鍵K<sub>temp</sub>で暗号化されたバックアップ鍵K<sub>ic</sub>を、SAM62に送信し、SAM62は、一時鍵K<sub>temp</sub>で暗号化されたバックアップ鍵K<sub>ic</sub>を復号する。ステップS159において、SAM62は、復号されたバックアップ鍵K<sub>ic</sub>で、ステップS152においてICカード55から読み出された古いレシーバ51の記憶モジュール73のデータ（SAMのID番号、保存用鍵K<sub>save</sub>及びHDD52のIDを示すバックアップデータ）を復号し、記憶モジュール73

に記憶させる。ステップS 1 6 0において、E M Dサービスセンタ 1のユーザ管理部 1 8は、I Cカード 5 5にデータを記憶させた古い装置のS A M 6 2のI Dに対応するユーザ登録データベース（図 7）のデータを登録不可に設定し、処理を終了する。

図 4 9に示した読み込みの処理は、図 4 3に示した処理に比較し、レシーバ 5 1とE M Dサービスセンタ 1の送受信されるデータの量が少なくでき、したがって、通信時間を短くできる。図 4 8のステップS 1 4 8において、図 4 9のステップS 1 5 7と同様に、E M Dサービスセンタ 1は、課金の処理を行ってもよい。

次に、図 4 7に示す処理でバックアップされたデータ読み出す場合の処理を、図 5 0に示すフローチャートを用いて説明する。ステップS 1 6 1において、新しいレシーバ 5 1のS A M 6 2の相互認証モジュール 7 1は、I Cカード 5 5の相互認証モジュール 8 0と相互認証する。この認証処理は、図 4 0乃至図 4 2を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 6 2において、S A M 6 2は、I Cカードインタフェース 6 4を介して、E M Dサービスセンタ 1の公開鍵  $K_{p e s c}$ で暗号化されている古いレシーバ 5 1の記憶モジュール 7 3のデータ（S A MのI D番号、保存用鍵  $K_{s a v e}$ 及びH D D 5 2のI Dを示すバックアップデータ）を読み出す。

ステップS 1 6 3において、S A M 6 2の相互認証モジュール 7 1は、通信部 6 1を介して、E M Dサービスセンタ 1の相互認証部 1 7と相互認証する。この認証処理は、図 4 0乃至図 4 2を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 6 4において、S A M 6 2は、通信部 6 1を介して、E M

Dサービスセンタ 1 の公開鍵  $K_{pesc}$  で暗号化されている記憶モジュール 7 3 のデータを、EMD サービスセンタ 1 のユーザ管理部 1 8 に送信する。

ステップ S 1 6 5 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、受信した記憶モジュール 7 3 のデータを自分自身の秘密鍵  $K_{sec}$  で復号する。ステップ S 1 6 6 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、復号したバックアップデータを、相互認証部 1 7 から供給された一時鍵  $K_{temp}$  で、再度、暗号化する。ステップ S 1 6 7 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、一時鍵  $K_{temp}$  で暗号化されたバックアップデータを、レシーバ 5 1 の通信部 6 1 に送信する。

ステップ S 1 6 8 において、レシーバ 5 1 の通信部 6 1 は、EMD サービスセンタ 1 のユーザ管理部 1 8 から受信したデータを、SAM 6 2 に送信し、SAM 6 2 は、そのデータを復号した後、記憶モジュール 7 3 に記憶させる。ステップ S 1 6 9 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、IC カード 5 5 にデータを記憶させた古い装置の SAM 6 2 の ID に対応するユーザ登録データベース (図 7) のデータを登録不可に設定する。

このように、図 4 7 に示す処理を用いたバックアップの場合、図 5 0 に示す処理により、新しいレシーバ 5 1 は、IC カード 5 5 のバックアップデータを読み込む。

レシーバ 5 1 は、自分自身を登録する場合 (図 3 7 のステップ S 1 2 に対応する処理を実行する場合)、図 4 3 のフローチャートに示す処理を実行するが、レシーバ 5 1 に従属するレコーダ 5 3 を EMD サービスセンタ 1 に登録する場合、図 5 1 のフローチャートに

示す処理を実行する。ステップS 1 8 1において、レシーバ5 1のSAM 6 2は、記憶モジュール7 3に記憶された登録リストに、レコーダ5 3のIDを書き込む。ステップS 1 8 2において、レシーバ5 1の相互認証モジュール7 1は、EMDサービスセンタ1の相互認証部1 7と相互認証する。この認証処理は、図4 0乃至図4 2を参照して説明した場合と同様であるので、ここでは説明を省略する。

ステップS 1 8 3において、EMDサービスセンタ1のユーザ管理部1 8は、レシーバ5 1のID（図4 4に示すSAM 6 2の証明書に含まれるSAM 6 2のID）を基に、ユーザ登録データベースを検索し、レシーバ5 1が登録不可であるか否かを判定し、レシーバ5 1が登録不可ではないと判定された場合、ステップS 1 8 4に進み、レシーバ5 1のSAM 6 2は、EMDサービスセンタ1のユーザ管理部1 8に、記憶モジュール7 3に記憶している配送用鍵K dのバージョン、課金情報（後述の図5 6に示すフローチャートのステップS 3 3 7の処理で記憶される）、登録リスト及び必要に応じて取扱方針を一時鍵K t e m pで暗号化し、通信部6 1を介して、EMDサービスセンタ1のユーザ管理部1 8に送信する。ステップS 1 8 5において、EMDサービスセンタ1のユーザ管理部1 8は、受信したデータを復号した後、課金情報を処理し、図4 5を参照して説明した、レシーバ5 1から受信した登録リストのレコーダ5 3に関する登録拒絶フラグ及びステータスフラグなどのデータの部分を更新し、レシーバ5 1に対応するデータに応じた署名を付する。なお、ここではデータを一時鍵K t e m pで暗号化して送付しているが、勿論暗号化しなくても良い。

ステップS 1 8 6において、E M D サービスセンタ 1 のユーザ管理部 1 8 は、レシーバ 5 1 が有する配送用鍵 K d のバージョンが最新か否かを判定し、レシーバ 5 1 が有する配送用鍵 K d のバージョンが最新であると判定された場合、ステップS 1 8 7に進み、一時鍵 K d で暗号化した、更新した登録リスト及び課金情報受信メッセージを、レシーバ 5 1 に送信し、レシーバ 5 1 は、更新した登録リスト及び課金情報受信メッセージを受信し、復号した後、記憶する。ステップS 1 8 8において、レシーバ 5 1 は、記憶モジュール 7 3 に記憶された課金情報を消去し、登録リストを、E M D サービスセンタ 1 のユーザ管理部 1 8 からステップS 1 8 7において受信したものに更新し、ステップS 1 9 1に進む。

ステップS 1 8 6において、レシーバ 5 1 が有する配送用鍵 K d のバージョンが最新のものではないと判定された場合、ステップS 1 8 9に進み、E M D サービスセンタ 1 のユーザ管理部 1 8 は、一時鍵 K d で暗号化した、最新バージョンの配送用鍵 K d、更新した登録リスト及び課金情報受信メッセージを、レシーバ 5 1 に送信し、レシーバ 5 1 は、最新バージョンの配送用鍵 K d、更新した登録リスト及び課金情報受信メッセージを受信し、復号した後、記憶する。ステップS 1 9 0において、レシーバ 5 1 は、記憶モジュール 7 3 に記憶された課金情報を消去し、登録リストを、E M D サービスセンタ 1 のユーザ管理部 1 8 からステップS 1 8 9において受信したものに更新し、配送用鍵 K d を最新バージョンのものに更新し、ステップS 1 9 1に進む。

ステップS 1 9 1において、レシーバ 5 1 のS A M 6 2 は、更新した登録リストを参照し、レコーダ 5 3 が登録不可か否かを判定し、

レコーダ 5 3 が登録不可でないと判定された場合、ステップ S 1 9 2 に進み、レシーバ 5 1 とレコーダ 5 3 は相互認証し、一時鍵 K t e m p を共有する。この認証処理は、図 4 0 乃至図 4 2 を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S 1 9 3 において、レコーダ 5 3 に、一時鍵 K d で暗号化した、登録完了メッセージ及び配送用鍵 K d を送信し、レコーダ 5 3 は、登録完了メッセージ及び配送用鍵 K d を受信し、復号する。ステップ S 1 9 4 において、レコーダ 5 3 は、配送用鍵 K d を更新し、処理は終了する。

ステップ S 1 8 3 においてレシーバ 5 1 が登録不可であると判定された場合、及び、ステップ S 1 9 1 においてレコーダ 5 3 が登録不可であると判定された場合、処理は終了する。

以上のように、レシーバ 5 1 に従属するレコーダ 5 3 は、レシーバ 5 1 を介して、EMD サービスセンタ 1 に登録される。

図 5 2 は、図 3 7 のステップ S 1 3 において、EMD サービスセンタ 1 がレシーバ 5 1 に送信した配送用鍵 K d を、レシーバ 5 1 が受け取る処理の詳細を説明するフローチャートである。ステップ S 2 0 1 において、レシーバ 5 1 の相互認証モジュール 7 1 は、EMD サービスセンタ 1 の相互認証部 1 7 と相互認証する。この認証処理は、図 4 0 乃至図 4 2 を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S 2 0 2 において、レシーバ 5 1 の S A M 6 2 は、通信部 6 1 を介して、EMD サービスセンタ 1 のユーザ管理部 1 8 に証明書を送信し、EMD サービスセンタ 1 のユーザ管理部 1 8 は、証明書を受信する。ステップ S 2 0 3 乃至ステップ S 2 1 0 は、図 5 1 のステップ S 1 8 3 乃至ステップ S 1 9



0と同様の処理であるのでその説明は省略する。

このように、レシーバ51は、EMDサービスセンタ1のユーザ管理部18から配送用鍵Kdを受け取り、レシーバ51の課金情報をEMDサービスセンタ1のユーザ管理部18に送信する。

次に、ユーザネットワーク5が図10又は図11の構成を有する場合、レシーバ51に従属するレコーダ53の配送用鍵Kdの受取処理（図45に示すステータスフラグが、レコーダ53の配送用鍵Kdの受取を許可する値を有する場合）を、図53に示すフローチャートを用いて説明する。ステップS221において、レシーバ51の相互認証モジュール71及びレコーダ53の図示せぬ相互認証モジュールは、相互認証する。この認証処理は、図40乃至図42を参照して説明した場合と同様であるので、ここでは説明を省略する。

ステップS222において、レシーバ51は、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っているか否かを判定し、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っていると判定された場合、ステップS223に進み、レシーバ51の記憶モジュール73に記憶する登録リストを基に、レコーダ53が登録不可であるか否かを判定する。ステップS223において、レコーダ53が登録不可ではないと判定された場合、ステップS224に進み、レコーダ53のSAM66は、レシーバ51のSAM62に、内蔵する記憶モジュールに記憶している配送用鍵Kd（後述する図53のステップS235でレシーバ51から受け取っている）のバージョン及び課金情報（後述する図56に対応する処理のステップS33

7に相当する処理で記憶している)を一時鍵K t e m pで暗号化して、送信し、レシーバ51のSAM62は、配送用鍵K dのバージョン及び課金情報を受信し、復号する。

ステップS225において、レシーバ51の相互認証モジュール71は、通信部61を介して、EMDサービスセンタ1の相互認証部17と、相互認証する。この認証処理は、図40乃至図42を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS226において、EMDサービスセンタ1のユーザ管理部18は、レシーバ51のIDを基に、ユーザ登録データベースを検索し、レシーバ51が登録不可であるか否かを判定し、レシーバ51が登録不可ではないと判定された場合、ステップS227に進み、レシーバ51のSAM62は、通信部61を介して、EMDサービスセンタ1のユーザ管理部18に、一時鍵K t e m pで暗号化した、記憶モジュール73に記憶している配送用鍵K dのバージョン、課金情報、登録リスト及び必要に応じて取扱方針並びにレコーダ53の課金情報を送信する。ステップS228において、EMDサービスセンタ1のユーザ管理部18は、受信したデータを復号した後、課金情報を処理し、図45で説明した、レシーバ51から受信した登録リストのレコーダ53に関する登録拒絶フラグ、ステータスフラグなどのデータの部分を更新し、レシーバ51に対応するデータに応じた署名を付する。

ステップS229乃至ステップS234の処理は、図51に示すステップS186乃至ステップS191とそれぞれ同様であるので、その説明は省略する。

ステップS234において、レシーバ51のSAM62は、更新

した登録リストを参照し、レコーダ53が登録不可か否かを判定し、レコーダ53が登録不可でないと判定された場合、ステップS235に進み、レコーダ53に、一時鍵Ktempで暗号化した、課金情報受信メッセージ及び配送用鍵Kdを送信し、レコーダ53は、課金情報受信メッセージ及び配送用鍵Kdを受信し、復号する。ステップS236において、レコーダ53のSAM66は、内蔵する記憶モジュールに記憶している、課金情報を消去し、配送用鍵Kdを最新のバージョンに更新する。

ステップS222において、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っていないと判定された場合、ステップS237に進み、図51に示したレコーダ53の登録処理を実行し、ステップS224に進む。

ステップS223においてレコーダ53が登録不可であると判定された場合、ステップS226においてレシーバ51が登録不可であると判定された場合、及び、ステップS234においてレコーダ53が登録不可であると判定された場合、処理は終了する。

以上のように、レシーバ51に従属するレコーダ53は、レシーバ51を介して、配送用鍵Kdを受け取る。

次に、図37のステップS14に対応する、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテンツを送信する処理を、図54のフローチャートを用いて説明する。ステップS251において、コンテンツプロバイダ2のウォータマーク付加部32は、コンテンツサーバ31から読み出したコンテンツに、コンテンツプロバイダ2を示す所定データ（例えばコンテンツプロバイダIDなど）をウォータマークとして付加し、圧縮部3

3に供給する。ステップS 2 5 2において、コンテンツプロバイダ2の圧縮部3 3は、ウォーターマークが挿入されたコンテンツをA T R A C等の所定の方式で圧縮し、暗号化部3 4に供給する。ステップS 2 5 3において、乱数発生部3 5は、コンテンツ鍵K c oとして用いる乱数を発生させ、暗号化部3 4に供給する。ステップS 2 5 4において、コンテンツプロバイダ2の暗号化部3 4は、D E Sなどの所定の方式で、コンテンツ鍵K c oを使用して、ウォーターマークが挿入され、圧縮されたコンテンツを暗号化する。

ステップS 2 5 5において、暗号化部3 6は、D E Sなどの所定の方式で、図3 7のステップS 1 1の処理により、E M Dサービスセンタ1から供給されている配送用鍵K dでコンテンツ鍵K c oを暗号化する。ステップS 2 5 6において、コンテンツプロバイダ2のセキュアコンテナ作成部3 8は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K c o及びポリシー記憶部3 7から供給された取扱方針にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵K s c pで暗号化し、図1 3に示すような署名を作成する。ステップS 2 5 7において、コンテンツプロバイダ2のセキュアコンテナ作成部3 8は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K c o、ポリシー記憶部3 7から供給される取扱方針及びステップS 2 5 6で生成した署名を含んだ、図1 3に示すようなコンテンツプロバイダセキュアコンテナを作成する。

ステップS 2 5 8において、コンテンツプロバイダ2の相互認証部3 9は、サービスプロバイダ3の相互認証部4 5と相互認証する。この認証処理は、図4 0乃至図4 2を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 2 5 9において、

コンテンツプロバイダ2のセキュアコンテナ作成部38は、サービスプロバイダ3に、コンテンツプロバイダセキュアコンテナに、予め認証局から発行してもらった証明書を付して送信し、処理を終了する。

以上のように、コンテンツプロバイダ2は、サービスプロバイダ3に、コンテンツプロバイダセキュアコンテナを送信する。

次に、図37のステップS15に対応する、サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアコンテナを送信する処理の詳細を図55のフローチャートを用いて説明する。ステップS291において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダ2のセキュアコンテナ作成部38から送信されたコンテンツプロバイダセキュアコンテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、コンテンツプロバイダ2の公開鍵K<sub>pcp</sub>を取り出す。証明書の署名の確認は、図42のステップS83における処理と同様であるので、その説明は省略する。

ステップS292において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダ2のセキュアコンテナ作成部38から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ2の公開鍵K<sub>pcp</sub>で復号し、得られたハッシュ値が、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K<sub>co</sub>及び取扱方針にハッシュ関数を適用し得られたハッシュ値と一致することを確認し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。改竄が発見された場合は、処理を終了する。コンテンツプロバイダセキュアコンテナに改竄がない場合、ステ

ステップS 2 9 3において、サービスプロバイダ3の値付け部4 2は、コンテンツプロバイダセキュアコンテナから取り扱い方針を取り出す。ステップS 2 5 4において、サービスプロバイダ3の値付け部4 2は、取扱方針を基に、図1 7で説明した価格情報を作成する。ステップS 2 9 5において、サービスプロバイダ3のセキュアコンテナ作成部4 4は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K c o、取扱方針、価格情報並びにこれらデータにハッシュ関数を適用して得られたハッシュ値を、自分自身の秘密鍵K s s pで暗号化し、得られた値を署名として図1 5に示すようなサービスプロバイダセキュアコンテナを作成する。

ステップS 2 9 6において、サービスプロバイダ3の相互認証部4 5は、レシーバ5 1の相互認証モジュール7 1と相互認証する。この認証処理は、図4 0乃至図4 2を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 2 9 7において、サービスプロバイダ3のセキュアコンテナ作成部4 4は、レシーバ5 1の通信部6 1に、証明書を付したサービスプロバイダセキュアコンテナを送信し、処理を終了する。

このように、サービスプロバイダ3は、レシーバ5 1にサービスプロバイダセキュアコンテナを送信する。

ユーザネットワーク5が図1 0又は図1 1の構成を有するときの、図3 7のステップS 1 6に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、レシーバ5 1の課金処理の詳細を、図5 6のフローチャートを用いて説明する。ステップS 3 3 1において、レシーバ5 1の復号/暗号化モジュール7 4は、配送用鍵K dでコンテンツ鍵K c oを復号できるか否かを判定し、配送用鍵K

dでコンテンツ鍵K c oを復号できないと判定された場合、ステップS 3 3 2で、レシーバ5 1は、図5 2で説明した配送用鍵K dの受取処理を実行し、ステップS 3 3 3に進む。ステップS 3 3 1において、配送用鍵K dでコンテンツ鍵K c oを復号できると判定された場合、ステップS 3 3 3に進む。ステップS 3 3 3において、レシーバ5 1の復号ユニット9 1は、図3 7のステップS 1 3の処理により、記憶モジュール7 3に記憶されている配送用鍵K dで、コンテンツ鍵K c oを復号する。

ステップS 3 3 4において、レシーバ5 1の課金処理モジュール7 2は、サービスプロバイダセキュアコンテナに含まれる取扱方針及び価格情報を取り出し、図1 9及び図2 0で説明した課金情報及び使用許諾情報を生成する。ステップS 3 3 5において、レシーバ5 1の課金処理モジュール7 2は、記憶モジュール7 3に記憶している課金情報及びステップS 3 3 4で算出された課金情報から、現在の課金が課金の上限以上であるか否かを判定し、現在の課金が課金の上限以上であると判定された場合、ステップS 3 3 6に進み、レシーバ5 1は図5 2で説明した配送用鍵K dの受取処理を実行し、新たな配送用鍵K dを受け取り、ステップS 3 3 7に進む。ステップS 3 3 5において、現在の課金が課金の上限未満であると判定された場合、ステップS 3 3 7に進む。

ステップS 3 3 7において、レシーバ5 1の課金処理モジュール7 2は、記憶モジュール7 3に課金情報を記憶させる。ステップS 3 3 8において、レシーバ5 1の課金処理モジュール7 2は、ステップS 3 3 4にて生成した使用許諾情報をH D D 5 2に記録する。ステップS 3 3 9において、レシーバ5 1のS A M 6 2は、H D D

52にサービスプロバイダセキュアコンテナから取り出した取扱方針を記録させる。

ステップS340において、レシーバ51の復号／暗号化モジュール74は、使用許諾情報にハッシュ関数を適用しハッシュ値を算出する。ステップS341において、レシーバ51の記憶モジュール73は、使用許諾情報のハッシュ値を記憶する。記憶モジュール73に保存用鍵Ksaveが記憶されていない場合、ステップS342において、レシーバ51の乱数発生ユニット92は、保存用鍵Ksaveである乱数を発生し、ステップS343に進む。記憶モジュール73に保存用鍵Ksaveが記憶されている場合、ステップS343に進む。

ステップS343において、レシーバ51の暗号化ユニット93は、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化する。ステップS344において、レシーバ51のSAM62は、暗号化されたコンテンツ鍵KcoをHDD52に記憶させる。記憶モジュール73に保存用鍵Ksaveが記憶されていない場合、ステップS345において、レシーバ51の復号／暗号化モジュール74は、保存用鍵Ksaveを記憶モジュール73に記憶させ、処理は終了する。記憶モジュール73に保存用鍵Ksaveが記憶されている場合、処理は終了する。

以上のように、レシーバ51は、課金情報を記憶モジュール73に記憶するとともに、コンテンツ鍵Kcoを配送用鍵Kdで復号し、再度、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化し、HDD52に記録させる。保存用鍵Ksaveは、記憶モジュール73に記憶される。



レコーダ 5 3 も、同様の処理で、課金情報を S A M 6 6 内の記憶モジュールに記憶するとともに、コンテンツ鍵 K c o を配送用鍵 K d で復号し、再度、コンテンツ鍵 K c o を保存用鍵 K s a v e で暗号化し、H D D 5 2 に記録させる。保存用鍵 K s a v e は、S A M 6 6 内の記憶モジュールに記憶される。なお、レシーバ 5 1 とレシーバ 5 3 においてそれぞれ保持される保存用鍵 K s a v e は、通常、違う鍵データとされている。

ユーザネットワーク 5 が図 2 8 の構成を有し、記憶モジュール 7 3 に検査値を記憶する場合の、図 3 7 のステップ S 1 5 及びステップ S 1 6 に対応する、レシーバ 5 1 の、適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を、図 5 7 のフローチャートを用いて説明する。ステップ S 3 6 1 において、レシーバ 5 1 の相互認証モジュール 7 1 は、通信部 6 1 を介して、サービスプロバイダ 3 の相互認証部 4 4 と相互認証し、相互認証できたとき、通信部 6 1 は、相互認証したサービスプロバイダ 3 から、サービスプロバイダセキュアコンテナを受信する。相互認証できなかった場合、処理は終了する。ステップ S 3 6 2 において、通信部 6 1 は、ステップ S 3 6 1 で相互認証したサービスプロバイダ 3 から、公開鍵証明書を受信する。

ステップ S 3 6 3 において、復号／暗号化モジュール 6 2 は、ステップ S 3 6 1 で受信したサービスプロバイダセキュアコンテナに含まれる署名データを検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了する。ステップ S 3 6 4 において、レシーバ 5 1 は、図示せぬ表示部に受信したサービスプロバイダセキュアコンテナに含まれる取扱い情報及び価格情報を

表示し、ユーザは、コンテンツの再生又はコピーなど、購入の内容を決定し、レシーバ51にその内容を指示する。ステップS365において、レシーバ51の課金処理モジュール72は、取扱い情報及び価格情報並びに購入の内容を基に、課金情報及び使用許諾情報を生成する。

ステップS366において、SAM62は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵Kcで暗号化されているコンテンツをHDD52に記録させる。ステップS367において、復号／暗号化ユニット74の復号ユニット91は、サービスプロバイダセキュアコンテナに含まれる配送用鍵Kdで暗号化されているコンテンツ鍵Kcを、図43のステップS110又は図52のステップS210で記憶モジュール73に記憶している配送用鍵Kdで復号する。ステップS368において、暗号化ユニット93は、ステップS367で復号されたコンテンツ鍵を記憶モジュール73に記憶している保存用鍵Ksで暗号化する。

ステップS369において、データ検査モジュール114は、外部記憶部113の、空きを有する鍵データブロックを検索する。ステップS370において、データ検査モジュール114は、ステップS369で検索した鍵データブロックに記憶されているデータ（コンテンツ鍵Kc、コンテンツIDなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップS371において、データ検査モジュール114は、ステップS370で得られたハッシュ値と、記憶モジュール73に記憶されている、ステップS369で検索された鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブ

ロックのデータは改竄されていないので、ステップS 3 7 2に進み、S A M 6 2は、ステップS 3 6 8にて暗号化されたコンテンツ鍵K c oを、外部記憶部1 1 3の空きを有する鍵データブロックに記憶させる。

ステップS 3 7 3において、復号／暗号化モジュール7 4は、外部記憶部1 1 3の、コンテンツ鍵K c oを記憶させた鍵データブロックに記憶しているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップS 3 7 4において、復号／暗号化モジュール7 4は、ステップS 3 7 3にて算出したハッシュ値を、記憶モジュール7 3の、コンテンツ鍵K c oを記憶させた鍵データブロックに対応する検査値に上書きする。ステップS 3 7 5において、課金モジュール7 2は、ステップS 3 6 5で作成した課金情報を記憶モジュール7 3に記憶させ、処理は終了する。

ステップS 3 7 1において、ステップS 3 7 0で得られたハッシュ値と、記憶モジュール7 3に記憶されている、ステップS 3 6 9で検索された鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、手続は、ステップS 3 7 6に進み、データ検査モジュール1 1 4は、外部記憶部1 1 3のすべての鍵データブロックを調べたか否かを判定し、外部記憶部1 1 3のすべての鍵データブロックを調べていないと判定された場合、ステップS 3 7 7に進み、データ検査モジュール1 1 4は、外部記憶部1 1 3の、他の空きを有する鍵データブロックを検索し、ステップS 3 7 0に戻り、処理を繰り返す。

ステップS 3 7 6において、外部記憶部1 1 3のすべての鍵デー

タブロックを調べたと判定された場合、コンテンツ鍵K c oを記憶できる鍵データブロックはないので、処理は終了する。

このように、図28のレシーバ51は、外部記憶部113のコンテンツ鍵K c o等が記憶されている鍵データブロックの改竄を検査し、改竄のない鍵データブロックのみに、新たなコンテンツ鍵K c oを記憶する。

ユーザネットワーク5が図28の構成を有し、外部記憶部113に検査値を記憶する場合の、図37のステップS15及びステップS16に対応する、レシーバ51の、適正なサービスプロバイダセキュリティコンテナを受信し、課金する処理の詳細を、図58のフローチャートを用いて説明する。ステップS391乃至ステップS400の処理は、図57のステップS361乃至ステップS370の処理とそれぞれ同様であり、その説明は省略する。

ステップS401において、復号ユニット91は、外部記憶部113に記憶されている、ステップS399で検索した鍵データブロックに対応する検査値を、記憶モジュール73に記憶する検査用鍵K c hで復号する。ステップS402において、データ検査モジュール114は、ステップS400で得られたハッシュ値と、ステップS401で復号された検査値とを比較し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、手続は、ステップS403に進む。

ステップS403及びステップS404の処理は、図57のステップS372及びステップS373の処理とそれぞれ同様であり、その説明は省略する。

ステップS405において、暗号化ユニット93は、ステップS

404において得られたハッシュ値を、記憶モジュール73に記憶する検査用鍵K<sub>ch</sub>で暗号化する。ステップS406において、復号／暗号化モジュール74は、ステップS405にて暗号化したハッシュ値を、記憶モジュール73の、コンテンツ鍵K<sub>co</sub>を記憶させた鍵データブロックに対応する検査値に上書きする。

ステップS407乃至ステップS409の処理は、図57のステップS375乃至ステップS377の処理とそれぞれ同様であり、その説明は省略する。

このように、図58に示す処理においても、図28のレシーバ51は、外部記憶部113のコンテンツ鍵K<sub>co</sub>等が記憶されている鍵データブロックの改竄を検査し、改竄のない鍵データブロックのみに、新たなコンテンツ鍵K<sub>co</sub>を記憶する。

図37のステップS17に対応するレシーバ51がコンテンツを再生する処理の詳細を、図59のフローチャートを用いて説明する。ステップS411において、レシーバ51の復号／暗号化モジュール74は、HDD52から、図56のステップS338で記憶した使用許諾情報及びステップS344で記憶した暗号化されたコンテンツ鍵K<sub>co</sub>を読み出す。ステップS412において、レシーバ51の復号／暗号化モジュール74は、使用許諾情報にハッシュ関数を適用しハッシュ値を算出する。

ステップS413において、レシーバ51の復号／暗号化モジュール74は、ステップS412において算出されたハッシュ値が、図56のステップS340で記憶モジュール73に記憶されたハッシュ値と一致するか否かを判定し、ステップS412において算出されたハッシュ値が、記憶モジュール73に記憶されたハッシュ値

と一致すると判定された場合、ステップS 4 1 4に進み、使用回数の値などの使用許諾情報に含まれる所定の情報を更新する。ステップS 4 1 5において、レシーバ5 1の復号／暗号化モジュール7 4は、更新した使用許諾情報にハッシュ関数を適用しハッシュ値を算出する。ステップS 4 1 6において、レシーバ5 1の記憶モジュール7 3は、ステップS 4 1 5で算出した使用許諾情報のハッシュ値を記憶する。ステップS 4 1 7において、レシーバ5 1の復号／暗号化モジュール7 4は、HDD 5 2に更新した使用許諾情報を記録させる。

ステップS 4 1 8において、SAM 6 2の相互認証モジュール7 1と伸張部6 3の相互認証モジュール7 5は、相互認証し、SAM 6 2及び伸張部6 3は、一時鍵K t e m pを記憶する。この認証処理は、図4 0乃至図4 2を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R 1、R 2又はR 3が、一時鍵K t e m pとして用いられる。ステップS 4 1 9において、復号／暗号化モジュール7 4の復号ユニット9 1は、図5 6のステップS 3 4 4にてHDD 5 2に記録されたコンテンツ鍵K c oを、記憶モジュール7 3に記憶された保存用鍵K s a v eで復号する。ステップS 4 2 0において、復号／暗号化モジュール7 4の暗号化ユニット9 3は、復号されたコンテンツ鍵K c oを一時鍵K t e m pで暗号化する。ステップS 4 2 1において、SAM 6 2は、一時鍵K t e m pで暗号化されたコンテンツ鍵K c oを伸張部6 3に送信する。

ステップS 4 2 2において、伸張部6 3の復号モジュール7 6は、コンテンツ鍵K c oを一時鍵K t e m pで復号する。ステップS 4

23において、SAM62は、HDD52に記録されたコンテンツを読み出し、伸張部63に送信する。ステップS424において、伸張部63の復号モジュール76は、コンテンツをコンテンツ鍵Kcoで復号する。ステップS425において、伸張部63の伸張モジュール78は、復号されたコンテンツをATRA Cなどの所定の方式で伸張する。ステップS426において、伸張部63のウォーターマーク付加モジュール79は、伸張されたコンテンツにレシーバ51を特定する所定のウォーターマークを挿入する。ステップS427において、レシーバ51は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

ステップS413において、ステップS412において算出されたハッシュ値が、記憶モジュール73に記憶されたハッシュ値と一致しないと判定された場合、ステップS428において、SAM62は、図示せぬ表示装置にエラーメッセージを表示させるなどの所定のエラー処理を実行し、処理は終了する。

このように、レシーバ51は、コンテンツを再生する。

図60は、図11の構成を有するユーザホームネットワーク5において、レシーバ51がデコーダ56にコンテンツを再生させる処理を説明するフローチャートである。ステップS431乃至ステップS437の処理は、図59のステップS411乃至ステップS417の処理とそれぞれ同様であるので、その説明は省略する。

ステップS438において、SAM62の相互認証モジュール71とデコーダ56の相互認証モジュール101は、相互認証し、一時鍵Ktempが共有される。この認証処理は、図40乃至図42を参照して説明した場合と同様であるので、ここでは説明を省略す

る。相互認証に用いられる乱数R 1、R 2又はR 3が、一時鍵K t e m pとして用いられる。ステップS 4 3 9において、復号／暗号化モジュール7 4の復号ユニット9 1は、H D D 5 2に記録されたコンテンツ鍵K c oを、記憶モジュール7 3に記憶された保存用鍵K s a v eで復号する。ステップS 4 4 0において、復号／暗号化モジュール7 4の暗号化ユニット9 3は、復号されたコンテンツ鍵K c oを一時鍵K t e m pで暗号化する。ステップS 4 4 1において、S A M 6 2は、一時鍵K t e m pで暗号化されたコンテンツ鍵K c oをデコーダ5 6に送信する。

ステップS 4 4 2において、デコーダ5 6の復号モジュール1 0 2は、コンテンツ鍵K c oを一時鍵K t e m pで復号する。ステップS 4 4 3において、S A M 6 2は、H D D 5 2に記録されたコンテンツを読み出し、デコーダ5 6に送信する。ステップS 4 4 4において、デコーダ5 6の復号モジュール1 0 3は、コンテンツをコンテンツ鍵K c oで復号する。ステップS 4 4 5において、デコーダ5 6の伸張モジュール1 0 4は、復号されたコンテンツをA T R A Cなどの所定の方式で伸張する。ステップS 4 4 6において、デコーダ5 6のウォータマーク付加モジュール1 0 5は、伸張されたコンテンツにデコーダ5 6を特定する所定のウォータマークを挿入する。ステップS 4 4 7において、デコーダ5 6は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

ステップS 4 4 8の処理は、図5 9のステップS 4 2 8の処理と同様であるので、その説明は省略する。

以上のように、ユーザホームネットワークが図1 1に示す構成を有する場合、レシーバ5 1が受信したコンテンツは、デコーダ5 6



で再生される。

図 6 7 は、本発明を適用した E M D システムの他の構成例を表している。なお、図中、図 1 及び図 1 0 における場合と対応する部分については、同一の符号を付してある。すなわち、この例においては、ユーザホームネットワーク 5 に代えて、ユーザホームネットワーク 2 0 0 が設けられ、そのユーザホームネットワーク 2 0 0 には、レコーダ 5 3 に代えて、レシーバ 2 0 1 及びレシーバ 2 0 2 が、レシーバ 5 1 に従属（接続）されている。

レシーバ 2 0 1 は、レシーバ 5 1 と同様の構成を有しており、レシーバ 5 1 の S A M 6 2 及び記憶モジュール 7 3 のそれぞれに対応する S A M 2 1 0 及び記憶モジュール 2 1 1 等を有し、そして H D D 2 0 3 に接続されている。レシーバ 2 0 2 も、レシーバ 5 1 と同様の構成を有しており、S A M 2 2 0 及び記憶モジュール 2 2 1 等を有している。レシーバ 2 0 2 は、レシーバ 2 0 1 にも接続（従属）する。ただし、レシーバ 2 0 2 は、H D D のような記録媒体には接続されていない。

レシーバ 5 1 は、図 1 0 に示す構成を有するが、この例において、S A M 6 2 の記憶モジュール 7 3 には、図 4 5 で示した登録リストに代えて、図 6 8 に示すような登録リストが記憶されている。この登録リストは、表形式に情報が記憶されているリスト部及び登録リストを保持する機器についての所定の情報が記憶されている対象 S A M 情報部より構成されている。

対象 S A M 情報部には、この登録リストを保有する機器の S A M I D、この例の場合、レシーバ 5 1 の S A M 6 2 の I D が（「対象 S A M I D」の欄に）記憶されている。対象 S A M 情報部にはまた、

この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ51には、レシーバ201及びレシーバ202の2機の機器が接続されているので、自分自身を含む合計値3が（「接続されている機器数」の欄に）記憶されている。

リスト部は、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態情報」、「登録条件署名」及び「登録リスト署名」の9個の項目から構成され、この例の場合、レシーバ51の登録条件、レシーバ201の登録条件及びレシーバ202の登録条件として、それぞれの項目に所定の情報が記憶されている。

「SAMID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ51のSAM62のID、レシーバ201のSAM210のID及びレシーバ202のSAM220のIDが記憶されている。「ユーザID」には、対応する機器（レシーバ51、レシーバ201及びレシーバ202）のユーザのユーザIDが記憶される。

「購入処理」には、対応する機器が、コンテンツを購入（具体的には、使用許諾条件やコンテンツ鍵Kcoを購入）するための処理を行うことができるか否かを示す情報（”可”又は”不可”）が記憶される。この例の場合、レシーバ51及びレシーバ201は、コンテンツを購入するための処理を行うことができるので、それぞれに対応する「購入処理」には、”可”が記憶されている。レシーバ202は、購入したコンテンツを記録する、例えば、HDDのよう

な記録媒体に接続されていないので、コンテンツを購入する処理を行うことができず、そのため、レシーバ202に対応する「購入処理」には、“不可”が記憶されている。

「課金処理」には、対応する機器が、EMDサービスセンタ1との間で、課金処理を行うことができるか否かを示す情報（“可”又は“不可”）が記憶される。なお、課金処理が行えるか否かは、EMDサービスセンタ1において、機器をEMDシステム登録する際に決定される。この例の場合、レシーバ51は、課金処理を行うことができる機器として登録されているので、対応する「課金処理」には、“可”が記憶されている。一方、レシーバ201及びレシーバ202は、この例の場合、課金処理を行うことができない機器として登録されているので、レシーバ201及びレシーバ202のそれぞれに対応する「課金処理」には、“不可”が記憶されている。なお、レシーバ202においては、コンテンツの購入がなされない所以、課金は計上されず、課金自体の必要がない。

「課金機器」には、対応する機器において計上された課金に対する課金処理を行う機器のSAMのIDが記憶される。この例の場合、レシーバ51（SAM62）は、自分自身の課金に対する課金処理を行うことができるので、その対応する「課金機器」には、レシーバ51のSAM62のIDが記憶されている。レシーバ51はまた、課金処理を行うことができないレシーバ201に代わり、レシーバ201により計上される課金に対する課金処理を行うので、レシーバ201に対応する「課金機器」には、レシーバ51のSAM62のIDが記憶されている。レシーバ202においては、上述したように、コンテンツが購入されず、課金も計上されない所以、レシー

バ 2 0 2 に対する課金処理は必要とされない。そのため、レシーバ 2 0 2 対応する「課金機器」には、課金処理を行う機器が存在しないことを示す情報（” なし” ）が記憶されている。

「コンテンツ供給機器」には、対応する機器が、コンテンツの供給をサービスプロバイダ 3 からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器の S A M の I D が記憶される。この例の場合、レシーバ 5 1 及びレシーバ 2 0 1 は、コンテンツの供給をサービスプロバイダ 3 から受けるので、それぞれに対応する「コンテンツ供給機器」には、コンテンツを供給する機器が存在しない旨を示す情報（” なし” ）が記憶されている。レシーバ 2 0 2 は、ネットワーク 4 に接続されていないことから、コンテンツの供給をサービスプロバイダ 3 から受けることができず、レシーバ 5 1 又はレシーバ 2 0 1 からコンテンツの供給を受ける。そのため、レシーバ 2 0 2 に対応する「コンテンツ供給機」には、レシーバ 5 1 の S A M 6 2 の I D 及びレシーバ 2 0 1 の S A M 2 1 0 の I D が記憶されている。

「状態情報」には、対応する機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（” 制限なし” ）、一定の制限が課せられている場合は、その旨を示す情報（” 制限あり” ）、また動作が停止される場合には、その旨を示す情報（” 停止” ）が記憶される。例えば、課金処理が成功しなかった場合、その機器に対応する「状態情報」には、” 制限あり” が設定される（詳細は後述する）。この例の場合、「状態情報」に” 制限あり” が設定された機器においては、既に購入されたコンテンツの再生（解説）処理は実行されるが、新たなコンテンツを購入するための

処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態情報」には、「停止」が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けうることができなくなる。

この例の場合、レシーバ51、レシーバ201及びレシーバ202に対して、何ら制限が課せられていないものとし、それぞれに対応する「状態情報」には、「制限なし」が設定されている。

「登録条件署名」には、上述したように、各機器（レシーバ51、レシーバ201及びレシーバ202）の登録条件として、それぞれ、「SAMID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態情報」及び「公開鍵」に記憶されている情報に対するEMDサービスセンタ1による署名が記憶されている。

「登録リスト署名」には、登録リストに設定されているすべてのデータに対する、EMDサービスセンタ1の署名が記憶されている。

図69は、レシーバ201のSAM210の記憶モジュール211に記憶されている、レシーバ201の登録リストを表している。この登録リストの対象SAM情報部には、レシーバ201のSAM210のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ201には、レシーバ51及びレシーバ202の2機が接続され、自分自身を含めた合計数3）が記憶されている。リスト部には、図68のレシーバ51の登録リストのリスト部と同様の情報が記憶されている。

図70は、レシーバ202のSAM220の記憶モジュール22

1に記憶されている、レシーバ202の登録リストを表している。この登録リストの対象SAM情報部には、レシーバ202のSAM220のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ202には、レシーバ51及びレシーバ201の2機が接続され、自分自身を含めた合計数3）が記憶されている。リスト部には、この例の場合、図68及び図69の登録リストのリスト部に登録されているレシーバ51、レシーバ201及びレシーバ202の登録条件のうち、レシーバ202の登録条件のみが記憶されている。

次に、図68、図69及び図70に示したそれぞれの登録リストを、レシーバ51の記憶モジュール73、レシーバ201の記憶モジュール211及びレシーバ202の記憶モジュール221に記憶させるための処理手順を、図71のフローチャートを参照して説明する。

ステップS501において、レシーバ51の登録処理が実行される。ステップS501における登録処理の詳細は、図72のフローチャートに示されている。

ステップS511乃至S518においては、図43のステップS101乃至S108における場合と同様の処理が実行されるので、その説明は省略するが、ステップS518において、EMDサービスセンタ1のユーザ管理部18は、ユーザ登録データベースに基づいて、図73に示すような登録リストを作成する。ここで作成された登録リストは、図68に示した登録リストにおいて、レシーバ51の登録条件のみが登録されているものに相当する。

ステップS519乃至S524においては、図43のステップS

109乃至S114における場合と同様の処理が実行されているので、その詳細の説明は省略するが、ステップS522において、レシーバ51のSAM62は、ステップS521で、EMDサービスセンタ1から送信された登録リストを、一時鍵Ktempで復号し、記憶モジュール73に記憶させる。このように、図73に示した登録リストが、レシーバ51の記憶モジュール73に記憶されたとき、処理は終了し、図71のステップS502に進む。

ステップS502において、レシーバ201及びレシーバ202の登録処理が実行される。ステップS502における登録処理の詳細は、図74のフローチャートに示されている。

ステップS531において、レシーバ51のSAM62は、HDD52に記憶されている登録リスト（図73）に、図75に示すように、レシーバ201のSAM210のID及びレシーバ202のSAM220のIDを「SAMID」に書き加え、そしてそれらに対応して、所定の情報を、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」の各項目に書き込む。

この例の場合、レシーバ201のSAM210のIDが設定された「SAMID」に対応して、「購入処理」に”可”が、「課金処理」に”不可”が、「課金機器」にレシーバ51のSAM62のIDが、そして「コンテンツ供給機器」に”なし”が書き込まれる。またレシーバ202のSAM220のIDが設定された「SAMID」に対応して、「購入処理」に”不可”が、「課金処理」に”不可”が、「課金機器」に”なし”が、そして「コンテンツ供給機器」にレシーバ51のSAM62のID及びレシーバ201のSAM210のIDが書き込まれる。なお、ここで、「購入処理」、

「課金処理」、「課金機器」及び「コンテンツ供給機器」のそれぞれに書き込まれる情報は、例えば、レシーバ201及びレシーバ202が、レシーバ51に接続される際に設定された条件により決定される。

次に、ステップS532において、レシーバ51とEMDサービスセンタ1との相互認証が行われる。この相互認証は、図40乃至図42を参照して説明した場合と同様の処理であるので、その説明は省略する。

ステップS533において、レシーバ51のSAM62は、HDD52に記憶されている、課金情報に関連した取扱方針を一時鍵Ktempで暗号化し、ステップS531で新たな情報が書き加えられた登録リスト、記憶モジュール73に記憶されている配送用鍵Kdのバージョン及び課金情報とともに、EMDサービスセンタ1に送信する。

ステップS534において、EMDサービスセンタ1のユーザ管理部18は、ステップS533で、レシーバ51から送信されてきた情報を受信し、復号する。その後、EMDサービスセンタ1のユーザ管理部18が、登録リストの「状態情報」に”停止”を設定すべき不正行為がレシーバ201及びレシーバ202において存在するか否かを確認する。

次に、ステップS535において、EMDサービスセンタ1のユーザ管理部18は、ユーザ登録データベースと、ステップS534でのユーザ管理部18による確認結果に基づいて、レシーバ201及びレシーバ202の登録条件を登録リストのリスト部に設定し、それに署名を付して、レシーバ51の登録リスト（図68）、を作



成し、そのリスト部の情報を記憶する。

次に、ステップS 5 3 6において、EMDサービスセンタ1のユーザ管理部18は、ステップS 5 3 5で作成された登録リスト（レシーバ51の登録リスト）を、一時鍵K t e m pで暗号化して、レシーバ51に送信する。

ステップS 5 3 7において、レシーバ51のSAM62は、ステップS 5 3 6で、EMDサービスセンタ1から送信された登録リストを受信し、復号した後、記憶モジュール73に記憶させる。これにより、ステップS 5 3 6で送信されてきたレシーバ51の登録リスト（図68）が、ステップS 5 2 2（図72）で記憶された図73に示した登録リストに代えて、記憶モジュール73に記憶される。これにより、処理は終了され、図71のステップS 5 0 3に進む。

ステップ503において、レシーバ51とレシーバ201の相互認証が行われるが、この相互認証処理は、図40乃至図42を参照して説明した場合と同様の処理であるので、その説明は省略する。

次に、ステップS 5 0 4において、レシーバ51のSAM62は、ステップS 5 3 7で記憶モジュール73に記憶された登録リストから、レシーバ201の登録リスト（図69）を生成してレシーバ201に送信する。

ステップS 5 0 5において、レシーバ201のSAM210は、ステップS 5 0 4でレシーバ51から送信された登録リストを受信し、復号した後、記憶モジュール211に記憶させる。これにより、図69に示した登録リストが、記憶モジュール211に記憶される。

次に、ステップ506において、レシーバ51とレシーバ202の相互認証が行われるが、この相互認証処理は、図40乃至図42

を参照して説明した場合と同様の処理であるので、その説明は省略する。

ステップS507において、レシーバ51のSAM62は、ステップS537で記憶モジュール73に記憶された登録リストのうち、レシーバ202の登録リスト（レシーバ202の登録条件のみが記憶されている登録リスト（図70））を、レシーバ202に送信する。

次に、ステップS508において、レシーバ202のSAM220は、ステップS507でレシーバ51から送信された登録リストを受信し、復号した後、記憶モジュール221に記憶させる。これにより、図70に示した登録リストが、記憶モジュール221に記憶される。その後、処理は終了される。

以上のようにして、レシーバ51、レシーバ201及びレシーバ202は、それぞれの登録リストを取得し、それを保持する。

次に、上述したように作成され、各レシーバに保持された登録リストの利用方法を、図56のフローチャートで説明した課金処理に対応させて説明する。

図56のフローチャートで説明された課金処理において、ステップS335で、現在の課金の合計が、予め設定された上限額以上であると判定された場合、ステップS336に進み、配送用鍵Kdの受取処理が実行される。この例の場合、図52のフローチャートで説明された手順に代わり、図76のフローチャートに示されている手順に従って処理が実行される。

すなわち、ステップS541において、レシーバ51とEMDサービスセンタ1との相互認証が行われる。この相互認証は、図40

乃至図42を参照して説明した場合と同様の処理であるので、その説明は省略する。

次に、ステップS542において、レシーバ51のSAM62は、必要に応じて、EMDサービスセンタ1のユーザ管理部18に証明書を送信する。ステップS543において、レシーバ51のSAM62は、HDD52に記憶されている、課金に関連する取扱方針を一時鍵Ktempで暗号化して、記憶モジュール73に記憶されている配送用鍵Kdのバージョン、課金情報及び登録リストとともに、EMDサービスセンタ1に送信する。

ステップS544において、EMDサービスセンタ1のユーザ管理部18は、ステップS543で、レシーバ51から送信された情報を受信し、復号した後、EMDサービスセンタ1の監査部21が、登録リストの「状態情報」に”停止”が設定されるべき不正行為がレシーバ51、レシーバ201及びレシーバ202において存在するか否かを確認する。

次に、ステップS545において、EMDサービスセンタ1のユーザ管理部18は、ステップS544での確認結果に基づいて、レシーバ51に不正行為が存在するか否かを判定し、レシーバ51に不正行為が存在しないと判定した場合、ステップS546に進む。

ステップS546において、EMDサービスセンタ1の課金請求部19は、ステップS543で受信された課金情報を解析し、ユーザの支払金額を算出する処理等を行う。次に、ステップS547において、EMDサービスセンタ1のユーザ管理部18は、ステップS546における処理により、決済が成功したか否かを確認し、その確認結果に基づいて、返却メッセージを作成する。この場合、レ

シーバ5 1 及びレシーバ2 0 1 の両者の課金に対する決済が共に成功したとき（すべての機器に対する決済が成功したとき）、成功返却メッセージが作成される。また、レシーバ5 1 又はレシーバ2 0 1 のいずれか一方の課金に対する決済が成功しなかったとき又はレシーバ5 1 及びレシーバ2 0 1 の両者の課金に対する決済が成功しなかったとき（すべての機器に対する決済が成功しなかったとき）、失敗返却メッセージが作成される。

次に、ステップS 5 4 8 において、EMDサービスセンタ1のユーザ管理部1 8 は、ユーザ登録データベース、ステップS 5 4 4 における不正行為が存在するか否かの確認結果及びステップS 5 4 7 における決済が成功したか否かの確認結果に基づいて、レシーバ5 1、レシーバ2 0 1 及びレシーバ2 0 2 の登録条件を設定し、それに署名を付して、登録リストをそれぞれ作成する。

例えば、ステップS 5 4 4 で、レシーバ2 0 1 又はレシーバ2 0 2 において不正行為が確認された場合、それらに対応する「状態情報」には” 停止” が設定され、この場合、今後、すべての処理が停止される。すなわち、EMDシステムからのサービスを一切受けることができなくなる。また、ステップS 5 4 7 で、決済が成功しなかったと確認された場合、「状態情報」には” 制限あり” が設定され、この場合、既に購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

次に、ステップS 5 4 9 に進み、EMDサービスセンタ1のユーザ管理部1 8 は、一時鍵K t e m p で、最新バージョンの配送用鍵K d（図3で示した3月分の最新バージョンの配送用鍵K d）及びステップS 5 4 8 で作成された登録リストを暗号化し、ステップS

5 4 7 で作成された返却メッセージとともにレシーバ 5 1 に送信する。

ステップ S 5 5 0 において、レシーバ 5 1 の S A M 6 2 は、ステップ S 5 4 9 で E M D サービスセンタ 1 から送信された情報を受信し、復号した後、記憶モジュール 7 3 に記憶させる。このとき、記憶モジュール 7 3 に記憶されていた課金情報は消去され、自分の登録リスト及び配送用鍵 K d は更新される。

次に、ステップ S 5 5 1 において、レシーバ 5 1 の S A M 6 2 は、ステップ S 5 5 0 で受信した返却メッセージが、成功返却メッセージであったか又は失敗返却メッセージであったかを判定し、成功返却メッセージであったと判定した場合、ステップ S 5 5 2 に進む。

ステップ S 5 5 2 において、レシーバ 5 1 の S A M 6 2 は、レシーバ 2 0 1 及びレシーバ 2 0 2 に対して、それぞれ相互認証処理（図 4 0 乃至図 4 2 を参照して説明した処理）を行った後、レシーバ 2 0 1 及びレシーバ 2 0 2 のそれぞれに、それぞれの登録リストと、配送用鍵 K d を送信する。

ステップ S 5 5 1 において、ステップ S 5 5 0 で受信した返却メッセージが、失敗返却メッセージであったと判定した場合、レシーバ 5 1 の S A M 6 2 は、ステップ S 5 5 3 に進み、ステップ S 5 4 1 で記憶モジュール 7 3 に記憶させた登録リスト（更新された登録リスト）を参照し、“制限あり”が「状態情報」に設定されているレシーバ（この例の場合、レシーバ 5 1 の自分自身又はレシーバ 2 0 1）を検出する。

次に、ステップ S 5 5 4 において、レシーバ 5 1 の S A M 6 2 は、ステップ S 5 5 0 で検出したレシーバに対して、所定の処理（R E

V O K E 処理) を実行し、そのレシーバにおいて実行される処理を制限する。すなわち、この場合、新たにコンテンツを購入するための処理が実行できないようにする。

ステップ S 5 4 5 において、レシーバ 5 1 において不正行為が確認された場合、ステップ S 5 5 5 に進み、EMD サービスセンタ 1 は、レシーバ 5 1、レシーバ 2 0 1 及びレシーバ 2 0 2 に対応する「状態情報」のすべてに” 停止” を設定し、登録リストを作成し、ステップ S 5 5 6 において、レシーバ 5 1 に送信する。なお、図 4 3 のフローチャートで示した登録処理を、レシーバ 2 0 1 又はレシーバ 2 0 2 に対して行うことより、レシーバ 2 0 1 又はレシーバ 2 0 2 におけるコンテンツの利用が可能となる。

次に、ステップ S 5 5 7 において、レシーバ 5 1 は、ステップ S 5 5 6 で EMD サービスセンタ 1 から送信された登録リストを受信し、登録リストを更新する。すなわち、この場合、配送用鍵 K d は、レシーバ 5 1、レシーバ 2 0 1 及びレシーバ 2 0 2 には、供給されず、レシーバ 5 1、レシーバ 2 0 1 及びレシーバ 2 0 2 は、供給されるコンテンツを再生することができなくなり、その結果、EMD システムにおけるサービスを一切受けることができなくなる。

ステップ S 5 5 2 において、レシーバ 2 0 1 及びレシーバ 2 0 2 に登録リスト及び配送用鍵 K d が送信されたとき、ステップ S 5 5 4 において、「状態情報」に” 制限あり” が設定されたレシーバに対して R E V O K E 処理が実行されたとき又はステップ S 5 5 7 において、「状態情報」に” 停止” が設定された登録リストに更新されたとき、処理は終了され、図 5 6 のステップ S 3 3 7 に進む。

ステップ S 3 3 7 乃至 S 3 4 5 における処理は、既に説明されて

いるので、ここでの説明は省略する。

以上のように、登録リストがEMDサービスセンタ1に送信されると（図76のステップS543）、EMDサービスセンタ1において、レシーバの不正行為が確認され、また処理（この例の場合、決済処理）が成功したか否かが確認され（ステップS547）、それらの確認結果に基づいて、登録リストが更新される。さらに、このようにして更新された登録リストは、各レシーバに保持されるようにしたので、各レシーバの動作を制御することができる。

以上においては、ステップS335において、計上された課金が予め設定された上限額を超えた場合、ステップS336に進み、配送用鍵Kdの受取処理が実行されるようにしたが、購入されるコンテンツの個数の上限数を設定し、購入されたコンテンツの個数がその上限数を超えた場合においても、ステップS336に進むようにすることもできる。

また、以上においては、課金処理における場合を例として、登録リストの利用方法を説明したが、コンテンツが復号される場合、取扱方針に含まれるコンテンツ鍵Kcoのバージョンが、レシーバ51のSAM62で保持される配送用鍵Kdのバージョンより新しいときなども、登録リストがレシーバ51よりEMDサービスセンタ1に送信される。この場合においても、登録リストは、上述したように、EMDサービスセンタ1において作成され、各レシーバにおいて配布される。

また、以上においては、機器（例えば、レシーバ51又はレシーバ201）が接続されるタイミングで、登録リストが課金情報とともにEMDサービスセンタ1に送信される場合を例として説明した

が、このとき登録リストのみが送信されるようにすることもできる。  
また、以上においては、機器が登録されるときに課金情報が、E M Dサービスセンタ 1 に送信される場合を例として説明したが、それ以外のタイミングで課金情報を E M D サービスセンタ 1 に送信するようにしてもよい。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、C D - R O M、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

次に、ユーザネットワーク 5 が図 2 8 の構成を有する場合の、M D ドライブ 5 4 から供給される暗号化されていないコンテンツを、暗号化し、記録する処理の詳細を、図 7 7 のフローチャートを用いて説明する。ステップ S 6 0 1 において、S A M 6 2 の乱数発生ユニット 9 2 は、乱数を生成し、コンテンツ鍵 K c o とする。ステップ S 6 0 2 において、通信部 6 1 は、M D ドライブ 5 4 から、M D ドライブ 5 4 に装着されている M D が記録するコンテンツを受信する。ステップ S 6 0 3 において、S A M 6 2 の暗号化ユニット 9 3 は、ステップ S 6 0 2 で受信したコンテンツを、ステップ S 6 0 1 で生成したコンテンツ鍵 K c o で暗号化する。ステップ S 6 0 4 において、S A M 6 2 は、暗号化されたコンテンツを H D D 5 2 に記録させる。ステップ S 6 0 5 において、S A M 6 2 の暗号化ユニット 9 3 は、コンテンツ鍵 K c o を記憶モジュール 7 3 に記憶している保存用鍵 K s a v e で暗号化する。



ステップS 6 0 6乃至ステップS 6 1 4の処理は、図5 7のステップS 3 6 9乃至ステップS 3 7 7の処理とそれぞれ同等であり、その説明は、省略する。

このように、レシーバ5 1は、MDドライブ5 4から供給される暗号化されていないコンテンツを、暗号化し、HDD 5 2に記録する。

図3 7のステップS 1 7に対応するレシーバ5 1がコンテンツを再生する処理の詳細を、図7 8のフローチャートを用いて説明する。ステップS 6 2 1において、レシーバ5 1の復号／暗号化モジュール7 4は、HDD 5 2から、図5 6のステップS 3 3 8で記憶した使用許諾情報及びステップS 3 4 4で記憶した暗号化されたコンテンツ鍵K c oを読み出す。ステップS 6 2 2において、レシーバ5 1の復号／暗号化モジュール7 4は、使用許諾情報にハッシュ関数を適用しハッシュ値を算出する。

ステップS 6 2 3において、レシーバ5 1の復号／暗号化モジュール7 4は、ステップS 6 2 2において算出されたハッシュ値が、図5 6のステップS 3 4 0で記憶モジュール7 3に記憶されたハッシュ値と一致するか否かを判定し、ステップS 6 2 2において算出されたハッシュ値が、記憶モジュール7 3に記憶されたハッシュ値と一致すると判定された場合、ステップS 6 2 4に進み、使用回数の値などの使用許諾情報に含まれる所定の情報を更新する。ステップS 6 2 5において、レシーバ5 1の復号／暗号化モジュール7 4は、更新した使用許諾情報にハッシュ関数を適用しハッシュ値を算出する。ステップS 6 2 6において、レシーバ5 1の記憶モジュール7 3は、ステップS 6 2 5で算出した使用許諾情報のハッシュ値

を記憶する。ステップS 6 2 7において、レシーバ5 1の復号／暗号化モジュール7 4は、H D D 5 2に更新した使用許諾情報を記録させる。

ステップS 6 2 8において、S A M 6 2の相互認証モジュール7 1と伸張部6 3の相互認証モジュール7 5は、相互認証し、S A M 6 2及び伸張部6 3は、一時鍵K t e m pを記憶する。この認証処理は、図4 0乃至図4 2を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R 1、R 2又はR 3が、一時鍵K t e m pとして用いられる。ステップS 6 2 9において、復号／暗号化モジュール7 4の復号ユニット9 1は、図5 6のステップS 3 4 4にてH D D 5 2に記録されたコンテンツ鍵K c oを、記憶モジュール7 3に記憶された保存用鍵K s a v eで復号する。ステップS 6 3 0において、復号／暗号化モジュール7 4の暗号化ユニット9 3は、復号されたコンテンツ鍵K c oを一時鍵K t e m pで暗号化する。ステップS 6 3 1において、S A M 6 2は、一時鍵K t e m pで暗号化されたコンテンツ鍵K c oを伸張部6 3に送信する。

ステップS 6 3 2において、伸張部6 3の復号モジュール7 6は、コンテンツ鍵K c oを一時鍵K t e m pで復号する。ステップS 6 3 3において、S A M 6 2は、H D D 5 2に記録されたコンテンツを読み出し、伸張部6 3に送信する。ステップS 6 3 4において、伸張部6 3の復号モジュール7 6は、コンテンツをコンテンツ鍵K c oで復号する。ステップS 6 3 5において、伸張部6 3の伸張モジュール7 8は、復号されたコンテンツをA T R A Cなどの所定の方式で伸張する。ステップS 6 3 6において、伸張部6 3のウォー

タマーク付加モジュール 7 9 は、伸張されたコンテンツにレシーバ 5 1 を特定する所定のウォータマークを挿入する。ステップ S 6 3 7 において、レシーバ 5 1 は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

ステップ S 6 2 3 において、ステップ S 6 2 2 において算出されたハッシュ値が、記憶モジュール 7 3 に記憶されたハッシュ値と一致しないと判定された場合、ステップ S 6 3 8 において、S A M 6 2 は、図示せぬ表示装置にエラーメッセージを表示させるなどの所定のエラー処理を実行し、処理は終了する。

このように、レシーバ 5 1 は、コンテンツを再生する。

図 7 9 は、図 1 1 の構成を有するユーザホームネットワーク 5 において、レシーバ 5 1 がデコーダ 5 6 にコンテンツを再生させる処理を説明するフローチャートである。ステップ S 6 4 1 乃至ステップ S 6 4 7 の処理は、図 7 8 のステップ S 6 2 1 乃至ステップ S 6 2 7 の処理とそれぞれ同様であるので、その説明は省略する。

ステップ S 6 4 8 において、S A M 6 2 の相互認証モジュール 7 1 とデコーダ 5 6 の相互認証モジュール 1 0 1 は、相互認証し、一時鍵 K t e m p が共有される。この認証処理は、図 4 0 乃至図 4 2 を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数 R 1、R 2 又は R 3 が、一時鍵 K t e m p として用いられる。ステップ S 6 4 9 において、復号／暗号化モジュール 7 4 の復号ユニット 9 1 は、H D D 5 2 に記録されたコンテンツ鍵 K c o を、記憶モジュール 7 3 に記憶された保存用鍵 K s a v e で復号する。ステップ S 6 5 0 において、復号／暗号化モジュール 7 4 の暗号化ユニット 9 3 は、復号されたコンテンツ鍵

K c oを一時鍵K t e m pで暗号化する。ステップS 6 5 1において、S A M 6 2は、一時鍵K t e m pで暗号化されたコンテンツ鍵K c oをデコーダ5 6に送信する。

ステップS 6 5 2において、デコーダ5 6の復号モジュール1 0 2は、コンテンツ鍵K c oを一時鍵K t e m pで復号する。ステップS 6 5 3において、S A M 6 2は、H D D 5 2に記録されたコンテンツを読み出し、デコーダ5 6に送信する。ステップS 6 5 4において、デコーダ5 6の復号モジュール1 0 3は、コンテンツをコンテンツ鍵K c oで復号する。ステップS 6 5 5において、デコーダ5 6の伸張モジュール1 0 4は、復号されたコンテンツをA T R A Cなどの所定の方式で伸張する。ステップS 6 5 6において、デコーダ5 6のウォータマーク付加モジュール1 0 5は、伸張されたコンテンツにデコーダ5 6を特定する所定のウォータマークを挿入する。ステップS 6 5 7において、デコーダ5 6は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

ステップS 6 5 8の処理は、図7 8のステップS 6 3 8の処理と同様であるので、その説明は省略する。

以上のように、ユーザホームネットワークが図1 1に示す構成を有する場合、レシーバ5 1が受信したコンテンツは、デコーダ5 6で再生される。

続いて、ユーザネットワーク5が図2 8の構成を有し、検査値が記憶モジュール7 3及び記憶部1 3 5に記憶されているときの、H D D 5 2に記録されているコンテンツを、レシーバ5 1に装着されているメモリスティック1 1 1に移動する処理を、図8 0及び図8 1のフローチャートを参照して説明する。ステップS 7 0 1におい

て、レシーバ 5 1 の相互認証モジュール 7 1 は、レシーバ 5 1 に装着されているメモリスティック 1 1 1 の相互認証部 1 3 3 と相互認証し、一時鍵  $K_{temp}$  を共有する。この認証処理は、図 4 0 乃至図 4 2 を参照して説明した場合と同様であるので、ここでは説明を省略する。

ステップ S 7 0 2 において、レシーバ 5 1 は、HDD 5 2 からコンテンツに関するデータを検索し、図示せぬ表示部に表示し、ユーザは、メモリスティック 1 1 1 に移動するコンテンツを選択し、レシーバ 5 1 に所定のデータを図示せぬスイッチで、入力する。ステップ S 7 0 3 において、レシーバ 5 1 の SAM 6 2 は、選択されたコンテンツに対応するコンテンツ鍵を、外部記憶部 1 1 3 から検索する。ステップ S 7 0 4 において、レシーバ 5 1 のデータ検査モジュール 1 1 4 は、移動するコンテンツに対応するコンテンツ鍵  $K_c$  を記憶する、外部記憶部 1 1 3 の鍵データブロックに記憶しているデータ（コンテンツ鍵  $K_c$ 、コンテンツ ID などのデータ）に、ハッシュ関数を適用し、ハッシュ値を得る。ステップ S 7 0 5 において、データ検査モジュール 1 1 4 は、ステップ S 7 0 4 で得られたハッシュ値と、記憶モジュール 7 3 に記憶されている、コンテンツ鍵  $K_c$  を記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップ S 7 0 6 に進み、レシーバ 5 1 の通信部 6 1 は、メモリスティック 1 1 1 の通信部 1 3 1 に書き込み要求コマンド及びコンテンツ ID を送信し、メモリスティック 1 1 1 の通信部 1 3 1 は、書き込み要求コマンド及びコンテンツ ID を受信する。

ステップS 7 0 7において、レシーバ5 1の通信部6 1は、メモリスティック1 1 1の通信部1 3 1にステップS 7 0 2で選択されたコンテンツを送信し、メモリスティック1 1 1の通信部1 3 1は、コンテンツを受信する。ステップS 7 0 8において、メモリスティック1 1 1のメモリコントローラ1 3 2は、通信部1 3 1が受信したコンテンツを、情報記憶ブロック1 2 2に、暗号化データ1 4 4として記憶させる。

ステップS 7 0 9において、レシーバ5 1の復号ユニット9 1は、コンテンツ鍵K c oを記憶モジュール7 3に記憶している保存用鍵K s a v eで復号し、暗号化ユニット9 3は、復号したコンテンツ鍵K c oを、一時鍵K t e m pで再度、暗号化し、S A M 6 2内の図示せぬレジスタに一時的に記憶する。ステップS 7 1 0において、S A M 6 2は、移動するコンテンツに対応する、外部記憶部1 1 3に記憶されているコンテンツ鍵K c oを削除する。ステップS 7 1 1において、レシーバ5 1の復号／暗号化モジュール7 4は、移動するコンテンツに対応するコンテンツ鍵K c oを削除した、外部記憶部1 1 3の鍵データブロックに記憶しているデータに、ハッシュ関数を適用し、ハッシュ値を得る。ステップS 7 1 2において、復号／暗号化モジュール7 4は、ステップS 7 1 1にて算出したハッシュ値を、記憶モジュール7 3の、コンテンツ鍵K c oを削除した鍵データブロックに対応する検査値に上書きする。

ステップS 7 1 3において、レシーバ5 1の通信部6 1は、コンテンツ鍵K c o、コンテンツI D及び使用許諾情報を、メモリスティック1 1 1の通信部1 3 1に送信し、メモリスティック1 1 1の通信部1 3 1は、コンテンツ鍵K c o、コンテンツI D及び使用許

諾情報を受信する。ステップS 7 1 4において、メモリスティック1 1 1の復号部1 3 6は、受信部1 3 1が受信したコンテンツ鍵K c oを一時鍵K t e m pで復号し、暗号化部1 3 4は、復号したコンテンツ鍵K c oを記憶部1 3 5が記憶する保存用鍵K s a v eで暗号化し、制御ブロック1 2 1内の図示せぬレジスタに一時的に記憶させる。

ステップS 7 1 5において、データ検査部1 3 8は、鍵データ1 4 3の、空きを有する鍵データブロックを検索する。ステップS 7 1 6において、データ検査部1 3 8は、ステップS 7 1 5で検索した鍵データブロックに記憶されているデータ（コンテンツ鍵K c o、コンテンツI Dなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップS 7 1 7において、データ検査部1 3 8は、ステップS 7 1 6で算出したハッシュ値と、記憶部1 3 5に記憶されている、ステップS 7 1 5で検索された鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していると判定された場合、ステップS 7 1 8に進み、メモリコントローラ1 3 2は、レジスタに一時的に記憶されているコンテンツ鍵K c oを、鍵データ1 4 3の空きのある鍵データブロックに記憶させる。

ステップS 7 1 9において、データ検査部1 3 8は、鍵データ1 4 3の、コンテンツ鍵K c oを記憶させた鍵データブロックに記憶しているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップS 7 2 0において、データ検査部1 3 8は、ステップS 7 1 9にて算出したハッシュ値を、記憶部1 3 5の、コンテンツ鍵K c oを記憶させた鍵データブロックに対応する検査値に上書きする。

ステップS 7 2 1において、メモリスティック1 1 1の通信部1

31は、レシーバ51の通信部61に、受信完了信号を送信し、レシーバ51の通信部61は、受信完了信号を受信する。ステップS722において、レシーバ51のSAM62は、HDD62からコンテンツを削除させ、コンテンツ鍵Kcoをレジスタから削除し、処理は終了する。

ステップS717において、ステップS716で得られたハッシュ値と、記憶部135に記憶されている、ステップS713で検索された鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、手続は、ステップS723に進み、データ検査部135は、鍵データ143のすべての鍵データブロックを調べたか否かを判定し、鍵データ143のすべての鍵データブロックを調べていないと判定された場合、ステップS724に進み、データ検査部135は、鍵データ143の、他の空きを有する鍵データブロックを検索し、ステップS716に戻り、処理を繰り返す。

ステップS723において、鍵データ143のすべての鍵データブロックを調べたと判定された場合、コンテンツ鍵Kcoを記憶できる鍵データブロックはないので、処理は終了する。

ステップS705において、データ検査モジュール114は、ステップS704で得られたハッシュ値と、記憶モジュール73に記憶されている、コンテンツ鍵Kcoを記憶している鍵データブロックに対応する検査値が一致しないと判定された場合、移動しようとしているコンテンツは改竄されているので、処理は終了する。

以上のように、HDD62に記憶されているコンテンツは、メモリスティック111に移動される。



ユーザネットワーク 5 が図 28 の構成を有し、検査値が外部記憶部 113 及び鍵データ 143 に記憶されているときの、HDD 52 に記録されているコンテンツを、レシーバ 51 に装着されているメモリスティック 111 に移動する処理を、図 82 及び図 83 のフローチャートを参照して説明する。ステップ S751 乃至ステップ S754 の処理は、図 80 のステップ S701 乃至ステップ S704 の処理とそれぞれ同様なので、その説明は省略する。

ステップ S755 において、データ検査モジュール 114 は、コンテンツ鍵 Kco を記憶している鍵データブロックに対応する検査値を記憶モジュール 73 が記憶する検査用鍵 Kch で復号する。ステップ S756 において、データ検査モジュール 114 は、ステップ S754 で得られたハッシュ値と、ステップ S755 で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップ S757 に進む。

ステップ S757 乃至ステップ S762 の処理は、図 80 のステップ S706 乃至ステップ S711 の処理とそれぞれ同様なので、その説明は省略する。

ステップ S763 において、暗号化ユニット 93 は、ステップ S762 で算出されたハッシュ値を、記憶モジュール 73 に記憶する検査用鍵 Kch で暗号化する。ステップ S764 において、復号／暗号化モジュール 74 は、ステップ S763 にて暗号化したハッシュ値を、外部記憶部 113 の、コンテンツ鍵 Kco を削除した鍵データブロックに対応する検査値に上書きする。

ステップ S765 乃至ステップ S768 の処理は、図 80 又は図

81のステップS713乃至ステップS716の処理とそれぞれ同様なので、その説明は省略する。

ステップS769において、復号部136は、ステップS767で検索した鍵データブロックに対応する検査値を記憶部135が記憶する検査用鍵Kchで復号する。ステップS770において、データ検査部138は、ステップS768で得られたハッシュ値と、ステップS769で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS771に進む。

ステップS771及びステップS772の処理は、図81のステップS718及びステップS719の処理と、それぞれ同様なので、その説明は省略する。

ステップS773において、データ検査部138は、ステップS772で算出されたハッシュ値を、記憶部135に記憶している検査用鍵Kchで暗号化する。ステップS774において、データ検査部138は、ステップS773にて暗号化したハッシュ値を、鍵データ143の、コンテンツ鍵Kcoを記憶させた鍵データブロックに対応する検査値に上書きする。

ステップS775乃至ステップS778の処理は、図81のステップS721乃至ステップS724の処理と、それぞれ同様なので、その説明は省略する。

ステップS756において、データ検査モジュール114は、ステップS754で得られたハッシュ値と、ステップS755で復号した検査値が一致しないと判定された場合、移動しようとしているコンテンツは改竄されているので、処理は終了する。

このように、HDD 6 2 に記憶されているコンテンツは、メモリスティック 1 1 1 に移動される。

次に、ユーザネットワーク 5 が図 2 8 の構成を有し、検査値が記憶モジュール 7 3 及び記憶部 1 3 5 に記憶されているときの、レシーバ 5 1 に装着されているメモリスティック 1 1 1 に記憶されているコンテンツを、HDD 5 2 に移動する処理を、図 8 4 及び図 8 5 のフローチャートを参照して説明する。ステップ S 7 9 1 において、レシーバ 5 1 の相互認証モジュール 7 1 は、レシーバ 5 1 に装着されているメモリスティック 1 1 1 の相互認証部 1 3 3 と相互認証し、一時鍵 K t e m p を共有する。この認証処理は、図 4 0 乃至図 4 2 を参照して説明した場合と同様であるので、ここでは説明を省略する。

ステップ S 7 9 2 において、レシーバ 5 1 は、通信部 6 1 を介して、メモリスティック 1 1 1 のデータ検索用テーブルからコンテンツに関するデータを検索し、図示せぬ表示部に表示し、ユーザは、HDD 5 2 に移動するコンテンツを選択し、レシーバ 5 1 に所定のデータを図示せぬスイッチで、入力する。ステップ S 7 9 3 において、レシーバ 5 1 の通信部 6 1 は、メモリスティック 1 1 1 の通信部 1 3 1 に移動要求コマンド及びコンテンツ ID を送信し、メモリスティック 1 1 1 の通信部 1 3 1 は、移動要求コマンド及びコンテンツ ID を受信する。

ステップ S 7 9 4 において、メモリスティック 1 1 1 のメモリコントローラ 1 3 2 は、受信したコンテンツ ID に対応したコンテンツ鍵 K c o を、鍵データ 1 4 3 から検索する。ステップ S 7 9 5 において、データ検査部 1 3 8 は、コンテンツ ID に対応したコンテ

ンツ鍵  $K_{co}$  を記憶している鍵データブロックに記憶されているデータ（コンテンツ鍵  $K_{co}$ 、コンテンツ ID などのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップ S 7 9 6 において、データ検査部 1 3 8 は、ステップ S 7 9 5 で算出したハッシュ値と、記憶部 1 3 5 に記憶されている、コンテンツ ID に対応したコンテンツ鍵  $K_{co}$  を記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していると判定された場合、コンテンツ鍵  $K_{co}$  などに改竄はないので、ステップ S 7 9 7 に進み、メモリコントローラ 1 3 2 は、データ検索用テーブル 1 4 1 を参照して、コンテンツ ID に対応したコンテンツを暗号化データ 1 4 4 から検索する。

ステップ S 7 9 8 において、メモリスティック 1 1 1 の通信部 1 3 1 は、レシーバ 5 1 の通信部 6 1 にステップ S 7 9 7 で検索されたコンテンツを送信し、レシーバ 5 1 の通信部 6 1 は、コンテンツを受信する。ステップ S 7 9 9 において、S A M 6 2 は、受信部 6 1 が受信したコンテンツを H D D 5 2 に記憶させる。

ステップ S 8 0 0 において、メモリスティック 1 1 1 の復号部 1 3 6 は、コンテンツ鍵  $K_{co}$  を記憶部 1 3 5 に記憶している保存用鍵  $K_{save}$  で復号し、暗号化部 1 3 4 は、復号したコンテンツ鍵  $K_{co}$  を、一時鍵  $K_{temp}$  で再度、暗号化し、制御ブロック 1 2 1 内の図示せぬレジスタに一時的に記憶する。ステップ S 8 0 1 において、メモリコントローラ 1 3 2 は、移動するコンテンツに対応する、鍵データ 1 4 3 に記憶されているコンテンツ鍵  $K_{co}$  を削除する。ステップ S 8 0 2 において、制御ブロック 1 2 1 のデータ検査部 1 3 8 は、移動するコンテンツに対応するコンテンツ鍵  $K_{co}$

を削除した、鍵データ 1 4 3 の鍵データブロックに記憶しているデータに、ハッシュ関数を適用し、ハッシュ値を得る。ステップ S 8 0 3 において、データ検査部 1 3 8 は、ステップ S 8 0 2 にて算出したハッシュ値を、鍵データ 1 4 3 の、コンテンツ鍵 K c o を削除した鍵データブロックに対応する検査値に上書きする。

ステップ S 8 0 4 において、メモリスティック 1 1 1 の通信部 1 3 1 は、コンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報を、レシーバ 5 1 の通信部 6 1 に送信し、レシーバ 5 1 の通信部 6 1 は、コンテンツ鍵 K c o、コンテンツ I D 及び使用許諾情報を受信する。ステップ S 8 0 5 において、レシーバ 5 1 のデータ検査モジュール 7 3 は、外部記憶部 1 1 3 の、空きを有する鍵データブロックを検索する。ステップ S 8 0 6 において、データ検査モジュール 1 1 4 は、ステップ S 8 0 5 で検索した鍵データブロックに記憶されているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップ S 8 0 7 において、データ検査モジュール 1 1 4 は、ステップ S 8 0 6 で得られたハッシュ値と、記憶モジュール 7 3 に記憶されている、ステップ S 8 0 5 で検索された鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップ S 8 0 8 に進み、レシーバ 5 1 の復号ユニット 9 1 は、受信部 6 1 が受信したコンテンツ鍵 K c o を一時鍵 K t e m p で復号し、暗号化ユニット 9 3 は、復号したコンテンツ鍵 K c o を記憶モジュール 7 3 が記憶する保存用鍵 K s a v e で暗号化する。ステップ S 8 0 9 に進み、S A M 6 2 は、ステップ S 8 0 7 にて暗号化されたコンテンツ鍵 K c o を、外部記憶部 1 1 3 の空きを有する鍵データプロ

ックに記憶させる。

ステップS 8 1 0において、復号／暗号化モジュール7 4は、外部記憶部1 1 3の、コンテンツ鍵K c oを記憶させた鍵データブロックに記憶しているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップS 8 1 1において、復号／暗号化モジュール7 4は、ステップS 8 1 0にて算出したハッシュ値を、記憶モジュール7 3の、コンテンツ鍵K c oを記憶させた鍵データブロックに対応する検査値に上書きする。ステップS 8 1 2において、レシーバ5 1の通信部6 1は、メモリスティック1 1 1の通信部1 3 1に受信完了信号を送信し、メモリスティック1 1 1の通信部1 3 1は、受信完了信号を受信する。ステップS 8 1 3において、メモリスティック1 1 1のメモリコントローラ1 3 2は、暗号化データ1 4 4から、送信したコンテンツを削除し、鍵データ1 4 3から、対応するコンテンツ鍵K c oを削除し、処理は終了する。

ステップS 8 0 7において、ステップS 8 0 6で得られたハッシュ値と、記憶モジュール7 3に記憶されている、ステップS 8 0 5で検索された鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、手続は、ステップS 8 1 4に進み、データ検査モジュール1 1 4は、外部記憶部1 1 3のすべての鍵データブロックを調べたか否かを判定し、外部記憶部1 1 3のすべての鍵データブロックを調べていないと判定された場合、ステップS 8 1 5に進み、データ検査モジュール1 1 4は、外部記憶部1 1 3の、他の空きを有する鍵データブロックを検索し、ステップS 8 0 6に戻り、処理を繰り返す。

ステップS 8 1 4において、外部記憶部 1 1 3のすべての鍵データブロックを調べたと判定された場合、コンテンツ鍵K c oを記憶できる鍵データブロックはないので、処理は終了する。

ステップS 7 9 6において、ステップS 7 9 5で算出したハッシュ値と、記憶部 1 3 5に記憶されている、コンテンツIDに対応したコンテンツ鍵K c oを記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していないと判定された場合、送信したいコンテンツのコンテンツ鍵K c oなどに改竄があるので、処理は終了する。

このように、コンテンツは、メモリスティック 1 1 1から、レシーバ5 1に移動される。

ユーザネットワーク 5が図 2 8の構成を有し、検査値が外部記憶部 1 1 3及び鍵データ 1 4 3に記憶されているときの、レシーバ5 1に装着されているメモリスティック 1 1 1に記憶されているコンテンツを、HDD 5 2に移動する処理を、図 8 6及び図 8 7のフローチャートを参照して説明する。ステップS 8 3 1乃至ステップS 8 3 5の処理は、図 8 4のステップS 7 9 1乃至ステップS 7 9 5の処理とそれぞれ同様なので、その説明は省略する。

ステップS 8 3 6において、復号部 1 3 6は、コンテンツ鍵K c oを記憶している鍵データブロックに対応する検査値を記憶部 1 3 5が記憶する検査用鍵K c hで復号する。ステップS 8 3 7において、データ検査部 1 3 8は、ステップS 8 3 5で得られたハッシュ値と、ステップS 8 3 6で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS 8 3 8に進む。

ステップS 8 3 8乃至ステップS 8 4 3の処理は、図8 4のステップS 7 9 7乃至ステップS 8 0 2の処理とそれぞれ同様なので、その説明は省略する。

ステップS 8 4 4において、データ検査部1 3 8は、ステップS 8 4 3で算出されたハッシュ値を、記憶部1 3 5に記憶する検査用鍵K c hで暗号化する。ステップS 8 4 5において、データ検査部1 3 8は、ステップS 8 4 4にて暗号化したハッシュ値を、鍵データ1 4 3の、コンテンツ鍵K c oを削除した鍵データブロックに対応する検査値に上書きする。

ステップS 8 4 6及びステップS 8 4 7の処理は、図8 5のステップS 8 0 4及びステップS 8 0 5の処理とそれぞれ同様なので、

ステップS 8 4 9において、データ検査モジュール1 1 4は、ステップS 8 4 7で検索した鍵データブロックに対応する検査値を記憶部1 3 5が記憶する検査用鍵K c hで復号する。ステップS 8 5 0において、データ検査モジュール1 1 4は、ステップS 8 4 8で得られたハッシュ値と、ステップS 8 4 9で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS 8 5 1に進む。

ステップS 8 5 1乃至ステップS 8 5 3の処理は、図8 5のステップS 8 0 8乃至ステップS 8 1 0の処理とそれぞれ同様なので、その説明は省略する。

ステップS 8 5 4において、暗号化ユニット9 3は、ステップS 8 5 5で算出されたハッシュ値を、記憶モジュール7 3に記憶している検査用鍵K c hで暗号化する。ステップS 8 5 5において、復



号／暗号化モジュール 7 4 は、ステップ S 8 5 4 にて暗号化したハッシュ値を、外部記憶部 1 1 3 の、コンテンツ鍵 K c o を記憶させた鍵データブロックに対応する検査値に上書きする。

ステップ S 8 5 6 乃至ステップ S 8 5 9 の処理は、図 8 5 のステップ S 8 1 2 乃至ステップ S 8 1 5 の処理と、それぞれ同様なので、その説明は省略する。

以上のように、検査値が外部記憶部 1 1 3 及び鍵データ 1 4 3 に記憶されているときでも、コンテンツは、メモリスティック 1 1 1 から、レシーバ 5 1 に移動される。

次に、ユーザネットワーク 5 が図 2 8 の構成を有し、検査値が記憶部 1 3 5 に記憶されているときの、レシーバ 5 1 に装着されているメモリスティック 1 1 1 に記憶されているコンテンツを、レシーバ 5 1 が再生する処理を、図 8 8 のフローチャートを参照して説明する。ステップ S 8 7 1 において、S A M 6 2 の相互認証モジュール 7 1 は、レシーバ 5 1 に装着されているメモリスティック 1 1 1 の相互認証部 1 3 3 と相互認証し、一時鍵 K t e m p を共有する。この認証処理は、図 4 0 乃至図 4 2 を参照して説明した場合と同様であるので、ここでは説明を省略する。コンテンツの再生におけるステップ S 8 7 1 の相互認証で使用する鍵は、図 8 4 に示すコンテンツの移動におけるステップ S 7 9 1 の相互認証で使用する鍵と、異なる鍵を使用してもよい。

ステップ S 8 7 2 において、レシーバ 5 1 の S A M 6 2 は、通信部 6 1 を介して、メモリスティック 1 1 1 のデータ検索用テーブルからコンテンツに関するデータを検索し、図示せぬ表示部に表示させ、ユーザは、再生するコンテンツを選択し、レシーバ 5 1 に所定

のデータを図示せぬスイッチで、入力する。ステップS 8 7 3において、レシーバ5 1のSAM 6 2は、通信部6 1を介して、メモリスティック1 1 1の通信部1 3 1に読み出し要求コマンド及びコンテンツIDを送信し、メモリスティック1 1 1の通信部1 3 1は、読み出し要求コマンド及びコンテンツIDを受信する。

ステップS 8 7 4において、メモリスティック1 1 1のメモリコントローラ1 3 2は、受信したコンテンツIDに対応したコンテンツ鍵K c oを、鍵データ1 4 3から検索する。ステップS 8 7 5において、データ検査部1 3 8は、コンテンツIDに対応したコンテンツ鍵K c oを記憶している鍵データブロックに記憶されているデータ（コンテンツ鍵K c o、コンテンツIDなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップS 8 7 6において、データ検査部1 3 8は、ステップS 8 7 5で算出したハッシュ値と、記憶部1 3 5に記憶されている、コンテンツIDに対応したコンテンツ鍵K c oを記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していると判定された場合、コンテンツ鍵K c oなどに改竄はないので、ステップS 8 7 7に進み、メモリコントローラ1 3 2は、データ検索用テーブル1 4 1を参照して、コンテンツIDに対応したコンテンツを暗号化データ1 4 4から検索する。

ステップS 8 7 8において、メモリスティック1 1 1の通信部1 3 1は、レシーバ5 1の通信部6 1にステップS 8 7 7で検索されたコンテンツを送信し、レシーバ5 1の通信部6 1は、コンテンツを受信する。ステップS 8 7 9において、メモリスティック1 1 1の復号部1 3 6は、コンテンツ鍵K c oを記憶部1 3 5に記憶して

いる保存用鍵K s a v eで復号し、暗号化部134は、復号したコンテンツ鍵K c oを、一時鍵K t e m pで再度、暗号化し、制御ブロック121内の図示せぬレジスタに一時的に記憶する。ステップS880において、メモリスティック111の通信部131は、コンテンツ鍵K c o、コンテンツID及び使用許諾情報を、レシーバ51のSAM62に送信し、レシーバ51のSAM62は、コンテンツ鍵K c o、コンテンツID及び使用許諾情報を受信する。

ステップS881において、SAM62の相互認証モジュール71は、伸張部63の相互認証モジュール75と相互認証し、一時鍵K t e m p（ステップS871で共有する一時鍵K t e m pとは異なる）を共有する。この認証処理は、図40乃至図42を参照して説明した場合と同様であるので、ここでは説明を省略する。

ステップS882において、SAM62の復号ユニット91は、コンテンツ鍵K c oを、メモリスティック111と共有している一時鍵K t e m pで復号し、暗号化ユニット93は、復号されたコンテンツ鍵K c oを、伸張部63と共有している一時鍵K t e m pで再度、暗号化する。ステップS883において、SAM62は、伸張部63と共有している一時鍵K t e m pで暗号化されたコンテンツ鍵K c oを、伸張部63に送信し、伸張部63は、暗号化されたコンテンツ鍵K c oを、受信する。

ステップS884において、伸張部63の復号モジュール76は、受信部61が受信したコンテンツ鍵K c oを、SAM62と共有する一時鍵K t e m pで復号する。ステップS885において、伸張部63の復号モジュール76は、ステップS878で受信したコンテンツを、ステップS884で復号したコンテンツ鍵K c oで復号

する。ステップS 8 8 6において、伸張部 6 3の伸張モジュール 7 8は、復号されたコンテンツをA T R A Cなどの所定の方式で伸張する。ステップS 8 8 7において、ウォータマーク付加モジュール 7 9は、伸張されたコンテンツにレシーバ 5 1を特定する所定のウォータマークを挿入する。ステップS 8 8 8において、伸張部 6 3は、図示せぬスピーカなどに再生されたコンテンツを出力する。ステップS 8 8 9において、レシーバ 5 1のS A M 6 2は、メモリスティック 1 1 1の通信部 1 3 1に再生完了信号を送信し、メモリスティック 1 1 1の制御ブロック 1 2 1は、再生完了信号を受信し、処理は終了する。

ステップS 8 7 6において、ステップS 8 7 5で算出したハッシュ値と、記憶部 1 3 5に記憶されている、コンテンツ I Dに対応したコンテンツ鍵 K c oを記憶している鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、コンテンツ鍵 K c oなどに改竄があるので、処理は終了する。

このように、鍵データブロックの改竄がないときのみ、レシーバ 5 1に装着されているメモリスティック 1 1 1に記憶されているコンテンツを、レシーバ 5 1は再生する。なお、ステップS 8 7 1において、伸張部 6 3とメモリスティック 1 1 1が、相互認証し、メモリスティック 1 1 1は、コンテンツ鍵 K c oを伸張部 6 3に直接送信し、伸張部 6 3はコンテンツ鍵 K c oを受信するようにしてもよい。

続いて、ユーザネットワーク 5が図 2 8の構成を有し、検査値が鍵データ 1 4 3に記憶されているとき、レシーバ 5 1に装着されているメモリスティック 1 1 1に記憶されているコンテンツを、レシ

ーバ51が再生する処理を、図89のフローチャートを参照して説明する。ステップS901乃至ステップS905の処理は、図88のステップS871乃至ステップS875の処理とそれぞれ同様なので、その説明は省略する。

ステップS906において、メモリスティック111の復号部136は、コンテンツ鍵Kcoを記憶している鍵データブロックに対応する検査値を記憶部135が記憶する検査用鍵Kchで復号する。ステップS907において、データ検査部131は、ステップS905で得られたハッシュ値と、ステップS906で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS908に進む。

ステップS908乃至ステップS920の処理は、図88のステップS877乃至ステップS889の処理とそれぞれ同様なので、その説明は省略する。

ステップS907において、ステップS905で得られたハッシュ値と、ステップS906で復号された検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、処理は終了する。

以上のように、暗号化されている検査値が鍵データ143に記憶されているときも、鍵データブロックの改竄がないときのみ、レシーバ51に装着されているメモリスティック111に記憶されているコンテンツを、レシーバ51は再生する。

図65を参照して後述する決済処理の前に行われる、EMDサービスセンタ1の決済オブジェクトを作成する処理を、図61のフロ

ーチャートを参照して説明する。ステップS 4 5 1において、E M Dサービスセンタ1の経歴データ管理部1 5は、図5 1のステップS 1 8 7又はステップS 1 8 9などでユーザホームネットワーク5から受信し、記憶した課金情報の中から、所定のコンテンツの利用に関する課金情報を選択し、選択した課金情報を利益分配部1 6に送信する。ステップS 4 5 2において、利益分配部1 6は、経歴データ管理部1 5から受信した課金情報にコンテンツプロバイダ2及びサービスプロバイダ3への利益配分を示すデータが含まれているか否かを判定し、経歴データ管理部1 5から受信した課金情報にコンテンツプロバイダ2及びサービスプロバイダ3への利益配分を示すデータが含まれていると判定された場合、ステップS 4 5 3に進む。

ステップS 4 5 3において、利益分配部1 6は、課金情報に含まれる利益配分を示すデータを参照して、所定のコンテンツを利用したユーザからサービスプロバイダ3への支払い金額を算出する。ステップS 4 5 4において、利益分配部1 6は、課金情報に含まれる利益配分を示すデータを参照して、サービスプロバイダ3からコンテンツプロバイダ2への支払い金額を算出する。ステップS 4 5 5において、利益分配部1 6は、課金情報に含まれる利益配分を示すデータを参照して、コンテンツプロバイダ2から権利団体への支払い金額を算出し、ステップS 4 5 9に進む。

ステップS 4 5 2において、経歴データ管理部1 5から受信した課金情報にコンテンツプロバイダ2及びサービスプロバイダ3への利益配分を示すデータが含まれていないと判定された場合、ステップS 4 5 6に進み、利益分配部1 6は、利益分配部1 6が記憶する

利益配分データベースを参照して、所定のコンテンツを利用したユーザからサービスプロバイダ3への支払い金額を算出する。ステップS457において、利益分配部16は、利益分配部16が記憶する利益配分データベースを参照して、サービスプロバイダ3からコンテンツプロバイダ2への支払い金額を算出する。ステップS458において、利益分配部16は、利益分配部16が記憶する利益配分データベースを参照して、コンテンツプロバイダ2から権利団体への支払い金額を算出し、ステップS459に進む。

ステップS459において、利益分配部16は、利益分配部16に記憶されている割引情報データベースのデータを参照して、所定のユーザからサービスプロバイダ3への支払い金額、サービスプロバイダ3からコンテンツプロバイダ2への支払い金額及びコンテンツプロバイダ2から権利団体への支払額を補正する。

ステップS460において、経歴データ管理部15は、すべてのコンテンツについてステップS453乃至ステップS459の計算を実行したか否かを判定し、すべてのコンテンツについてステップS453乃至ステップS459の計算をまだ実行していないと判定された場合、手続は、ステップS451に戻り、それ以降の処理を繰り返す。ステップS460において、すべてのコンテンツについてステップS451乃至ステップS459の計算が実行されたと判定された場合、手続は、ステップS461に進む。

ステップS461において、利益分配部16は、ユーザ毎に各サービスプロバイダ3への支払金額を算出し、クレジット決済オブジェクト1（例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図62（A）に示すクレジット決済オブジェクト

1) を作成する。クレジット決済オブジェクト 1 では、支払元にユーザの ID が設定され、支払先にサービスプロバイダ 3 の ID が設定され、支払額にサービスプロバイダ 3 への支払額が設定される。ステップ S 4 6 2 において、利益分配部 1 6 は、サービスプロバイダ 3 毎に各コンテンツプロバイダ 2 への支払金額を算出し、クレジット決済オブジェクト 2 (例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図 6 2 (B) に示すクレジット決済オブジェクト 2) を作成する。クレジット決済オブジェクト 2 では、支払元にクレジット決済オブジェクト 1 が設定され、支払先にコンテンツプロバイダ 2 の ID が設定され、支払額にコンテンツプロバイダ 2 への支払額が設定される。

ステップ S 4 6 3 において、利益分配部 1 6 は、コンテンツプロバイダ 2 毎に権利団体への支払金額を算出し、クレジット決済オブジェクト 3 (例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図 6 2 (C) に示すクレジット決済オブジェクト 3) を作成する。クレジット決済オブジェクト 3 では、支払元にクレジット決済オブジェクト 1 が設定され、支払先に権利団体の ID が設定され、支払額に権利団体への支払額が設定される。ステップ S 4 6 4 において、課金請求部 1 9 は、課金請求部 1 9 が記憶する、ユーザに対する EMD サービスセンタ 1 の利用料金を格納するユーザ利用料金テーブルを参照してユーザからの徴収金額を算出し、クレジット決済オブジェクト 4 (例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図 6 2 (D) に示すクレジット決済オブジェクト 4) を作成し、クレジット決済オブジェクト 1 の徴収額を設定し、処理を終了する。クレジット決済オブジェクト 4



では、支払元にクレジット決済オブジェクト 1 が設定され、支払先に EMD サービスセンタ 1 の I D が設定され、支払額に EMD サービスセンタ 1 への支払額が設定される。

以上のように、EMD サービスセンタ 1 は、決済オブジェクトを作成する。

図 6 3 は、サービスプロバイダ 3、コンテンツプロバイダ 2 及び権利団体が、EMD サービスセンタ 1 にサービス料を銀行決済で支払う場合の、銀行決済オブジェクトの例を示す図である。図 6 3

(A) の銀行決済オブジェクト 1 では、支払元にサービスプロバイダ 3 の I D が設定され、徴収額にサービスプロバイダ 3 からの徴収額が設定され、支払先に EMD サービスセンタ 1 の I D が設定され、支払額に EMD サービスセンタ 1 への支払額（徴収額と同額）が設定される。図 6 3 (B) の銀行決済オブジェクト 2 では、支払元にコンテンツプロバイダ 2 の I D が設定され、徴収額にコンテンツプロバイダ 2 からの徴収額が設定され、支払先に EMD サービスセンタ 1 の I D が設定され、支払額に EMD サービスセンタ 1 への支払額（徴収額と同額）が設定される。図 6 3 (C) の銀行決済オブジェクト 3 では、支払元に権利団体の I D が設定され、徴収額に権利団体からの徴収額が設定され、支払先に EMD サービスセンタ 1 の I D が設定され、支払額に EMD サービスセンタ 1 への支払額（徴収額と同額）が設定される。

図 6 4 は、ユーザがクレジットカードを利用して料金を支払い、サービスプロバイダ 3 及びコンテンツプロバイダ 2 は銀行口座を利用して決済を行う場合の、決済オブジェクトの例を示す図である。図 6 4 (A) 及び図 6 4 (D) のクレジット決済オブジェクトは、

図 6 2 (A) 及び図 6 2 (D) のクレジット決済オブジェクトとそれぞれ同様であり、その説明は省略する。図 6 4 (B) の銀行決済オブジェクト 2 は、支払元にサービスプロバイダ 3 の I D が設定され、徴収額に、コンテンツプロバイダ 2 への支払額と権利団体への支払額を合わせた、サービスプロバイダ 3 からの金額が設定され、支払先にコンテンツプロバイダ 2 の I D が設定され、支払額にコンテンツプロバイダ 2 への支払額（徴収額と同額）が設定される。図 6 4 (C) の銀行決済オブジェクト 3 は、支払元にコンテンツプロバイダ 2 の I D が設定され、徴収額に、コンテンツプロバイダ 2 からの徴収額が設定され、支払先に権利団体の I D が設定され、支払額に権利団体への支払額（徴収額と同額）が設定される。

図 6 2、図 6 3 及び図 6 4 の決済オブジェクトに記述された、支払元、徴収額、支払先及び支払金額に基づき、決済が実行されことにより、E M D サービスセンタ 1、コンテンツプロバイダ 2、サービスプロバイダ 3 及び権利団体に所定の金額が支払われる。E M D サービスセンタ 1 のクレジット決済処理オブジェクトを用いる決済の処理を図 6 5 のフローチャートを参照して説明する。ステップ S 4 7 1 において、E M D サービスセンタ 1 の出納部 2 0 は、クレジット決済オブジェクトの支払先に記載されている I D より、支払先の銀行などの決済機関を求める。ステップ S 4 7 2 において、E M D サービスセンタ 1 の出納部 2 0 は、クレジット決済オブジェクトの支払元に記載されている I D より、支払元のクレジット会社などの決済機関を求める。ステップ S 4 7 3 において、出納部 2 0 は、予め記憶された情報により、支払元の与信処理が必要であるか否かを判定し、支払元の与信処理が必要であると判定された場合、ステ

ステップS 4 7 4において、与信処理を実行する。ステップS 4 7 4の与信処理において、支払元が支払いできないと判定された場合、処理は終了する。ステップS 4 7 4の与信処理において、支払元が支払いできると判定された場合、ステップS 4 7 5に進む。

ステップS 4 7 3において、支払元の与信処理が必要でないと判定された場合、ステップS 4 7 5に進む。

ステップS 4 7 5において、出納部 2 0 は、前に実行された決済オブジェクトの処理が完了しているか否かを判定し、前に実行された決済オブジェクトの処理が完了していると判定された場合、ステップS 4 7 6に進み、ステップS 4 7 1 及びステップS 4 7 2 で求めた決済機関に、クレジット決済オブジェクトに記載された徴収額及び支払い金額に対応した決済命令を送信する。ステップS 4 7 7 において、クレジット決済オブジェクトの支払先に記載されているIDに対応する支払先にステップS 4 7 6 で実行した決済処理の情報を送信する。ステップS 4 7 8 において、クレジット決済オブジェクトの支払元に記載されているIDに対応する支払元にステップS 4 7 6 で実行した決済処理の情報を送信し、処理は終了する。

ステップS 4 7 5 において、前に実行された決済オブジェクトの処理が完了していないと判定された場合、ステップS 4 7 9 に進み、出納部 2 0 は、処理が完了していない決済オブジェクトに記載された支払元に所定のメッセージを送信するなどの、決済未完了の所定のエラー処理を実行し、処理は終了する。

以上のように、クレジット決済処理オブジェクトを用いる決済が処理される。

図 6 6 は、EMD サービスセンタ 1 の銀行決済処理オブジェクト

を用いる決済の処理を説明するフローチャートである。銀行決済処理オブジェクトを用いる決済の処理は、図65に示すクレジット決済処理オブジェクトを用いる決済の処理から、ステップS471及びステップS474の与信に関する処理を除いたものと同様である。ステップS481及びステップS482の処理は、図65のステップS471及びステップS472の処理とそれぞれ同様であるので、その説明は省略する。ステップS483乃至ステップS487の処理は、図65のステップS475乃至ステップS479の処理とそれぞれ同様であるので、その説明は省略する。

このように、銀行決済処理オブジェクトを用いる決済が処理され、クレジット決済処理オブジェクトを用いる決済の処理とともに、ユーザ、コンテンツプロバイダ2、サービスプロバイダ3及び権利団体から所定の金額が徴収され、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3及び権利団体に所定の金額が入金される。

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ又はプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG (Moving Picture Experts Group) などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT (商標) が提案するFEAL、IDEA (International Data Encryption Algorithm) 又は1ビット乃至数ビット単位

で暗号化するストリーム暗号などでもよい。

さらに、コンテンツ及びコンテンツ鍵K c oの暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

また、図5 1のステップS 1 8 4、図5 2のステップS 2 0 4及び図5 3のステップS 2 2 7において、レシーバ5 1は、EMDサービスセンタ1に課金情報を送信するとして説明したが、使用許諾情報の全部又は一部を送信するようにしてもよい。使用許諾情報には、ユーザが何の権利を買い取ったかが書き込まれているため、EMDサービスセンタ1は、使用許諾情報、価格情報及び取扱方針に含まれる情報をつき合わせるにより、決済処理が可能である。

また、図8 0のステップS 7 0 6、図8 2のステップS 7 5 7、図8 4のステップS 7 9 3、図8 6のステップS 8 3 3、図8 8のステップS 8 7 3及び図8 9のステップS 9 0 3において、レシーバ5 1は、メモリスティック1 1 1に送信するコマンドに、レシーバ5 1の秘密鍵で暗号化した署名を付して、メモリスティック1 1 1に送信し、メモリスティック1 1 1は、その署名を検査することにより、不正に対する耐性をより強化するようにしてもよい。

さらに、図8 0乃至図8 7のコンテンツの移動の処理において、コンテンツ鍵K c oは、再暗号化され、一時的に記憶された後、削除されるとして説明したが、コンテンツ鍵K c oを受け取る側が、コンテンツ鍵を記憶する領域がないなどの理由により、コンテンツ鍵K c oを削除し、コンテンツ鍵K c oを受け取れなかった場合の不都合を回避するために、コンテンツ鍵K c oを送る側は、受信完了信号を受信するまで、コンテンツ鍵K c oを一時的に使用不可（コンテンツ鍵K c oの状態を示すフラグを定義し、そのフラグを

使用するなどの処理をする)とし、受信完了信号を受信できなかったときは、そのコンテンツ鍵K<sub>co</sub>を再度、使用できるような処理を行っても良い。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星、ケーブルなどの通信媒体を利用することができる。

以上のように、本発明では、第1の鍵を第2の鍵で復号し、復号できなかったとき、第2の鍵の送信を要求するようにしたので、データ提供側が任意のタイミングで鍵を変更したとしても、ユーザが、常に、暗号化された情報を、確実に復号することができる。

また、本発明では、課金の値が所定の値に達したとき、第2の鍵の送信が要求されるようにしたので、データ提供側が任意のタイミングで鍵を変更したとしても、ユーザが、常に、暗号化された情報を、確実に復号することができる。

さらに、本発明では、情報処理装置を特定するデータを記憶し、情報処理装置を特定するデータを管理装置に送信し、情報処理装置を特定するデータを送信するとき、第2の鍵の送信が要求されるようにしたので、データ提供側が任意のタイミングで鍵を変更したとしても、ユーザが、常に、暗号化された情報を、確実に復号することができる。

本発明では、相互認証し、一時鍵を生成し、第2の鍵を記憶し、第2の鍵で第1の鍵を復号し、第1の鍵を一時鍵で暗号化し、一時

鍵で第1の鍵を復号し、第1の鍵で情報を復号するようにしたので、情報の復号のとき、情報を暗号化する鍵が読み出されない。

本発明では、情報提供装置が、暗号化された情報に、情報の取扱いを示す情報を付加して、情報配布装置に送信し、情報配布装置が、情報提供装置から送信された情報の取扱いを示す情報を基に、情報の使用料を算出し、暗号化された情報に、使用料を付加して、情報処理装置に送信し、情報処理装置が、使用料を基に、情報の利用に応じた課金情報を作成し、課金情報を、情報の取扱いを示す情報及び使用料の一部又は全部とともに、管理装置に送信し、管理装置が、課金情報、情報の取扱いを示す情報及び使用料の一部又は全部から不正を検出するようにしたので、正当な鍵を有する者の不当な価格付け又は取扱いの情報の改変などの不正を検出できるようになる。

また、本発明では、暗号化された情報に、情報の取扱いを示す情報を付加して、情報配布装置に送信し、受信した暗号化された情報及び情報の取扱いを示す情報を送信し、情報の取扱いを示す情報を基に、情報の利用に応じた使用許諾情報を作成し、使用許諾情報の取扱いを示す情報の一部又は全部とともに送信し、使用許諾情報及び情報の取扱いを示す情報の一部又は全部から不正を検出するようにしたので、正当な鍵を有する者の不当な価格付け又は取扱いの情報の改変などの不正を検出できるようになる。

本発明では、情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録するようにしたので、迅速にユーザの契約の可否が判断できるようになる。

また、本発明では、情報処理装置に従属する他の情報処理装置の

登録を請求するようにしたので、複数の情報処理装置を有するユーザも簡単に契約の処理ができるようになる。

また、本発明では、管理装置が、情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録し、情報処理装置が、情報処理装置に従属する他の情報処理装置の登録を請求するようにしたので、迅速にユーザの契約の可否が判断でき、複数の情報処理装置を有するユーザも簡単に契約の処理ができるようになる。

また、本発明では、登録条件を記憶するようにしたので、違反などがあった場合の動作を簡単かつ確実に制御（制限）することができる。

さらに、本発明では、所定の処理を実行するとき、登録条件を作成するようにしたので、違反などがあった場合の情報処理装置の動作を簡単にかつ確実に制御（制限）することができる。

本発明では、情報の使用の許諾条件を示す情報を生成し、許諾条件を示す情報の認証情報を生成し、認証情報を記憶するようにしたので、情報の使用の許諾条件の書換えを検出し、対応することができる。

また、本発明では、情報の利用のときに必要な関連情報の認証情報を生成し、認証情報を記憶し、関連情報から、他の認証情報を生成し、記憶している認証情報との一致を検証し、情報記憶媒体と相互認証するようにしたので、情報の関連情報の書換えを検出し、対応することができる。

また、本発明では、認証情報生成手段が、情報の利用のときに必要な関連情報の認証情報を生成し、記憶手段が認証情報を記憶し、



検証手段が、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証し、相互認証手段が、情報処理装置と相互認証するようにしたので、情報の関連情報の書換えを検出し、対応することができる。

本発明では、情報を特定するデータ及び情報の利用に対する情報提供業者の支払い金額を示すデータを記憶し、記憶するデータを基に、情報提供業者毎の支払い金額の合計を算出し、情報提供業者毎の利益を基に、決済機関に対し情報提供業者毎の決済を指示するようにしたので、精算処理及び利益の算出の処理が効率良くできるようになる。

本発明では、装着された外部記憶媒体と相互認証し、所定の鍵で所定の情報を暗号化するようにしたので、不正に対する安全性を保持したまま、必要な情報を外部に記憶できる。

また、本発明では、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号するようにしたので、不正に対する安全性を保持したまま、必要な情報を外部に記憶できる。

また、本発明では、情報処理装置が、装着された外部記憶媒体と相互認証し、管理装置の公開鍵で所定の情報を暗号化し、管理装置が、外部記憶媒体に記憶されたデータを復号するようにしたので、不正に対する安全性を保持したまま、必要な情報を外部に記憶できる。

さらに、本発明では、情報処理装置と相互認証するようにしたので、不正な読み取りを防止できる。

## 請求の範囲

1. 暗号化された情報、前記情報を復号する暗号化された第1の鍵及び前記第1の鍵を復号する第2の鍵を受信し、前記情報を復号する情報処理装置において、

前記第1の鍵を前記第2の鍵で復号する復号手段と、

前記復号手段が前記第1の鍵を復号できなかったとき、前記第2の鍵の送信を要求する要求手段と

を備えることを特徴とする情報処理装置。

2. 暗号化された情報、前記情報を復号する暗号化された第1の鍵及び前記第1の鍵を復号する第2の鍵を受信し、前記情報を復号する情報処理方法において、

前記第1の鍵を前記第2の鍵で復号する復号ステップと、

前記復号ステップで前記第1の鍵を復号できなかったとき、前記第2の鍵の送信を要求する要求ステップと

を含むことを特徴とする情報処理方法。

3. 暗号化された情報、前記情報を復号する暗号化された第1の鍵及び前記第1の鍵を復号する第2の鍵を受信し、前記情報を復号する情報処理装置に、

前記第1の鍵を前記第2の鍵で復号する復号ステップと、

前記復号ステップで前記第1の鍵を復号できなかったとき、前記第2の鍵の送信を要求する要求ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

4. 暗号化された情報、前記情報を復号する暗号化された第1の鍵及び前記第1の鍵を復号する第2の鍵を受信し、前記情報を復号する情報処理装置において、

課金のための処理を実行する課金手段と、

前記課金手段による課金の値が所定の値に達したとき、前記第2の鍵の送信を要求する要求手段と

を備えることを特徴とする情報処理装置。

5. 暗号化された情報、前記情報を復号する暗号化された第1の鍵及び前記第1の鍵を復号する第2の鍵を受信し、前記情報を復号する情報処理方法において、

課金のための処理を実行する課金ステップと、

前記課金ステップでの課金の値が所定の値に達したとき、前記第2の鍵の送信を要求する要求ステップと

を含むことを特徴とする情報処理方法。

6. 暗号化された情報、前記情報を復号する暗号化された第1の鍵及び前記第1の鍵を復号する第2の鍵を受信し、前記情報を復号する情報処理装置に、

課金のための処理を実行する課金ステップと、

前記課金ステップでの課金の値が所定の値に達したとき、前記第2の鍵の送信を要求する要求ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

7. 所定の管理装置が管理するシステムから、暗号化された情報、前記情報を復号する暗号化された第1の鍵及び前記第1の鍵を復号する第2の鍵を受信し、前記情報を復号する情報処理装置において、

前記情報処理装置を特定するデータを記憶する記憶手段と、  
前記情報処理装置を特定するデータを前記管理装置に送信する送信手段と、

前記情報処理装置を特定するデータを送信するとき、前記第 2 の鍵の送信を要求する要求手段と

を備えることを特徴とする情報処理装置。

8. 所定の管理装置が管理するシステムから、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を受信し、前記情報を復号する情報処理方法において、前記情報処理装置を特定するデータを記憶する記憶ステップと、前記情報処理装置を特定するデータを前記管理装置に送信する送信ステップと、

前記情報処理装置を特定するデータを送信するとき、前記第 2 の鍵の送信を要求する要求ステップと

を含むことを特徴とする情報処理方法。

9. 所定の管理装置が管理するシステムから、暗号化された情報、前記情報を復号する暗号化された第 1 の鍵及び前記第 1 の鍵を復号する第 2 の鍵を受信し、前記情報を復号する情報処理装置に、

前記情報処理装置を特定するデータを記憶する記憶ステップと、

前記情報処理装置を特定するデータを前記管理装置に送信する送信ステップと、

前記情報処理装置を特定するデータを送信するとき、前記第 2 の鍵の送信を要求する要求ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

10. 暗号化された情報、前記情報を復号する暗号化された第1の鍵及び前記第1の鍵を復号する第2の鍵を使用し、前記情報を復号する、第1の記憶手段及び第1の復号手段を有する情報処理装置において、

前記第1の記憶手段は、前記第1の復号手段と相互認証し、一時鍵を生成する第1の相互認証手段と、前記第2の鍵を記憶する第2の記憶手段と、前記第2の鍵で前記第1の鍵を復号する第2の復号手段と、前記第1の鍵を前記一時鍵で暗号化する暗号化手段とを備え、

前記第1の復号手段は、前記第1の記憶手段と相互認証し、一時鍵を生成する第2の相互認証手段と、前記一時鍵で前記第1の鍵を復号する第3の復号手段と、前記第1の鍵で前記情報を復号する第4の復号手段とを備える

ことを特徴とする情報処理装置。

11. 暗号化された情報、前記情報を復号する暗号化された第1の鍵及び前記第1の鍵を復号する第2の鍵を使用し、前記情報を復号する記憶手段及び復号手段を有する情報処理装置の情報処理方法において、

前記記憶手段は、前記復号手段と相互認証し、一時鍵を生成する第1の相互認証ステップと、

前記第2の鍵を記憶する記憶ステップと、

前記第2の鍵で前記第1の鍵を復号する第1の復号ステップと、

前記第1の鍵を前記一時鍵で暗号化する暗号化ステップとを含み、

前記復号手段は、前記記憶手段と相互認証し、一時鍵を生成する第2の相互認証ステップと、

前記一時鍵で前記第 1 の鍵を復号する第 2 の復号ステップと、  
前記第 1 の鍵で前記情報を復号する第 3 の復号ステップと  
を含むことを特徴とする情報処理方法。

1 2. 暗号化された情報、前記情報を復号する暗号化された第 1  
の鍵及び前記第 1 の鍵を復号する第 2 の鍵を使用し、前記情報を復  
号する記憶手段及び復号手段を有する情報処理装置の、

前記記憶手段に、前記復号手段と相互認証し、一時鍵を生成する  
第 1 の相互認証ステップと、

前記第 2 の鍵を記憶する記憶ステップと、

前記第 2 の鍵で前記第 1 の鍵を復号する第 1 の復号ステップと、

前記第 1 の鍵を前記一時鍵で暗号化する暗号化ステップとを含む  
処理を実行させ、

前記復号手段に、前記記憶手段と相互認証し、一時鍵を生成する  
第 2 の相互認証ステップと、

前記一時鍵で前記第 1 の鍵を復号する第 2 の復号ステップと、

前記第 1 の鍵で前記情報を復号する第 3 の復号ステップとを含む  
処理を実行させるコンピュータが読み取り可能なプログラムを提供  
する

ことを特徴とするプログラム提供媒体。

1 3. 暗号化された情報を提供する情報提供装置、前記提供され  
た情報を配布する情報配布装置、前記配布された情報を復号し利用  
する情報処理装置並びに前記情報提供装置、前記情報配布装置及び  
前記情報処理装置を管理する管理装置からなる情報提供システムに  
おいて、

前記情報提供装置は、前記暗号化された情報に、情報の取扱いを

示す情報を付加して、前記情報配布装置に送信する第 1 の送信手段を備え、

前記情報配布装置は、前記情報提供装置から送信された情報の取扱いを示す情報を基に、前記情報の使用料を算出する算出手段と、前記暗号化された情報に前記使用料を付加して、前記情報処理装置に送信する第 2 の送信手段とを備え、

前記情報処理装置は、前記使用料を基に前記情報の利用に応じた課金情報を作成する課金情報作成手段と、前記課金情報を、情報の取扱いを示す情報及び使用料の一部又は全部とともに、前記管理装置に送信する第 3 の送信手段とを備え、

前記管理装置は、前記課金情報、情報の取扱いを示す情報及び使用料の一部又は全部から不正を検出する検出手段を備える

ことを特徴とする情報提供システム。

14. 前記課金情報及び情報の取扱いを示す情報は、署名を付されて、送信されることを特徴とする請求の範囲第 13 項に記載の情報提供システム。

15. 前記課金情報及び情報の取扱いを示す情報は、暗号化されて送信されることを特徴とする請求の範囲第 13 項に記載の情報提供システム。

16. 暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムの情報提供方法において、

前記情報提供装置の情報提供方法は、前記暗号化された情報に、

情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第1の送信ステップを含み、

前記情報配布装置の情報提供方法は、前記情報提供装置から送信された情報の取扱いを示す情報を基に、前記情報の使用料を算出する算出ステップと、

前記暗号化された情報に、前記使用料を付加して、前記情報処理装置に送信する第2の送信ステップとを含み、

前記情報処理装置の情報提供方法は、前記使用料を基に、前記情報の利用に応じた課金情報を作成する課金情報作成ステップと、

前記課金情報を、情報の取扱いを示す情報及び使用料の一部又は全部とともに、前記管理装置に送信する第3の送信ステップとを含み、

前記管理装置の情報提供方法は、前記課金情報、情報の取扱いを示す情報及び使用料の一部又は全部から不正を検出する検出ステップ

を含むことを特徴とする情報提供方法。

17. 暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムの、

前記情報提供装置に、前記暗号化された情報に、情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第1の送信ステップを含む処理を実行させ、

前記情報配布装置に、前記情報提供装置から送信された情報の取扱いを示す情報を基に、前記情報の使用料を算出する算出ステップ



と、

前記暗号化された情報に、前記使用料を付加して、前記情報処理装置に送信する第2の送信ステップとを含む処理を実行させ、

前記情報処理装置に、前記使用料を基に、前記情報の利用に応じた課金情報を作成する課金情報作成ステップと、

前記課金情報を、情報の取扱いを示す情報及び使用料の一部又は全部とともに、前記管理装置に送信する第3の送信ステップとを含む処理を実行させ、

前記管理装置に、前記課金情報、情報の取扱いを示す情報及び使用料の一部又は全部から不正を検出する検出ステップ

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

18. 暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムにおいて、

前記情報提供装置は、前記暗号化された情報に、情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第1の送信手段を備え、

前記情報配布装置は、前記情報提供装置から受信した前記暗号化された情報及び前記情報の取扱いを示す情報を、前記情報処理装置に送信する第2の送信手段を備え、

前記情報処理装置は、前記情報の取扱いを示す情報を基に、前記情報の利用に応じた使用許諾情報を作成する使用許諾情報作成手段

と、前記使用許諾情報を、情報の取扱いを示す情報の一部又は全部とともに、前記管理装置に送信する第3の送信手段とを備え、

前記管理装置は、前記使用許諾情報及び情報の取扱いを示す情報の一部又は全部から不正を検出する検出手段を備える

ことを特徴とする情報提供システム。

19. 前記使用許諾情報及び情報の取扱いを示す情報は、署名を付されて、送信されることを特徴とする請求の範囲第18項に記載の情報提供システム。

20. 前記使用許諾情報及び情報の取扱いを示す情報は、暗号化されて、送信されることを特徴とする請求の範囲第18項に記載の情報提供システム。

21. 暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムの情報提供方法において、

前記情報提供装置の情報提供方法は、前記暗号化された情報に、情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第1の送信ステップを含み、

前記情報配布装置の情報提供方法は、前記情報提供装置から受信した前記暗号化された情報及び前記情報の取扱いを示す情報を、前記情報処理装置に送信する第2の送信ステップを含み、

前記情報処理装置の情報提供方法は、前記情報の取扱いを示す情報を基に、前記情報の利用に応じた使用許諾情報を作成する使用許諾情報作成ステップと、

前記使用許諾情報を、情報の取扱いを示す情報の一部又は全部とともに、前記管理装置に送信する第3の送信ステップとを含み、

前記管理装置の情報提供方法は、前記使用許諾情報及び情報の取扱いを示す情報の一部又は全部から不正を検出する検出ステップを含むことを特徴とする情報提供方法。

22. 暗号化された情報を提供する情報提供装置、前記提供された情報を配布する情報配布装置、前記配布された情報を復号し利用する情報処理装置並びに前記情報提供装置、前記情報配布装置及び前記情報処理装置を管理する管理装置からなる情報提供システムの、

前記情報提供装置に、前記暗号化された情報に、情報の取扱いを示す情報を付加して、前記情報配布装置に送信する第1の送信ステップを含む処理を実行させ、

前記情報配布装置に、前記情報提供装置から受信した前記暗号化された情報及び前記情報の取扱いを示す情報を、前記情報処理装置に送信する第2の送信ステップを含む処理を実行させ、

前記情報処理装置に、前記情報の取扱いを示す情報を基に、前記情報の利用に応じた使用許諾情報を作成する使用許諾情報作成ステップと、

前記使用許諾情報を、情報の取扱いを示す情報の一部又は全部とともに、前記管理装置に送信する第3の送信ステップとを含む処理を実行させ、

前記管理装置に、前記使用許諾情報及び情報の取扱いを示す情報の一部又は全部から不正を検出する検出ステップ

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

23. 暗号化された情報を提供する情報提供装置及び前記情報を利用する情報処理装置を管理する管理装置において、

前記情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に前記情報処理装置を登録する登録手段を備えることを特徴とする管理装置。

24. 前記データは、前記IDに対応して決済の可否を示すデータを含むことを特徴とする請求の範囲第23項に記載の管理装置。

25. 前記登録手段は、前記管理装置と通信する前記情報処理装置に従属する他の情報処理装置を登録することを特徴とする請求の範囲第23項に記載の管理装置。

26. 暗号化された情報を提供する情報提供装置及び前記情報を利用する情報処理装置を管理する管理方法において、

前記情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録ステップを含むことを特徴とする管理方法。

27. 暗号化された情報を提供する情報提供装置及び前記情報を利用する情報処理装置を管理する管理装置に、

前記情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録ステップ

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

28. 管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置において、

前記情報処理装置に従属する他の情報処理装置の登録を請求する

登録請求手段を備えることを特徴とする情報処理装置。

29. 前記情報処理装置は、前記情報処理装置に従属する他の情報処理装置の決済処理を代行する決済代行手段を更に備えることを特徴とする請求の範囲第28項に記載の情報処理装置。

30. 管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置の情報処理方法において、

前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップを含むことを特徴とする情報処理方法。

31. 管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置に、

前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップ

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

32. 暗号化されて提供される情報を復号し、利用する情報処理装置及び前記情報処理装置を管理する管理装置からなる情報利用システムにおいて、

前記管理装置は、前記情報処理装置のID及びそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置に登録する登録手段を備え、

前記情報処理装置は、前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求手段を備える

ことを特徴とする情報利用システム。

33. 管理装置に管理され、かつ、他の情報処理装置と接続され、暗号化された情報を復号し、利用する情報処理装置において、

前記管理装置及び前記他の情報処理装置と相互認証する相互認証手段と、

所定の情報を復号する復号化手段と、

前記管理装置により作成された登録条件を授受する授受手段と、

前記授受手段により授受された前記登録条件を記憶する記憶手段と、

前記記憶手段により記憶されている前記登録条件に基づいて、動作を制御する制御手段と

を備えることを特徴とする情報処理装置。

34. 管理装置に管理され、かつ、他の情報処理装置と接続され、暗号化された情報を復号し、利用する情報処理装置の情報処理方法において、

前記管理装置及び前記他の情報処理装置と相互認証する相互認証ステップと、

所定の情報を復号する復号化ステップと、

前記管理装置により作成された登録条件を授受する授受ステップと、

前記授受ステップで授受された前記登録条件を記憶する記憶ステップと、

前記記憶ステップで記憶された前記登録条件に基づいて、動作を制御する制御ステップと

を含むことを特徴とする情報処理方法。

35. 管理装置に管理され、かつ、他の情報処理装置と接続され、暗号化された情報を復号し、利用する情報処理装置に、

前記管理装置及び前記他の情報処理装置と相互認証する相互認証

ステップと、

所定の情報を復号する復号化ステップと、

前記管理装置により作成された登録条件を授受する授受ステップと、

前記授受ステップで授受された前記登録条件を記憶する記憶ステップと、

前記記憶ステップで記憶された前記登録条件に基づいて、動作を制御する制御ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

36. 暗号化された情報を復号し、利用する情報処理装置を管理する管理装置において、

前記情報処理装置に供給するデータを暗号化する暗号手段と、

前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行手段と、

前記実行手段により所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成手段と、

前記作成手段により作成された前記登録条件を前記情報処理装置に送信する送信手段と

を備えることを特徴とする管理装置。

37. 暗号化された情報を復号し、利用する情報処理装置を管理する管理装置の管理方法において、

前記情報処理装置に供給するデータを暗号化する暗号ステップと、

前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、

前記実行ステップで所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成ステップと、

前記作成ステップで作成された前記登録条件を前記情報処理装置に送信する送信ステップと

を含むことを特徴とする管理方法。

38. 暗号化された情報を復号し、利用する情報処理装置を管理する管理装置に、

前記情報処理装置に供給するデータを暗号化する暗号ステップと、  
前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、

前記実行ステップで所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成ステップと、

前記作成ステップで作成された前記登録条件を前記情報処理装置に送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

39. 暗号化されている情報を復号して利用する情報処理装置において、

前記情報の使用の許諾条件を示す情報を生成する許諾情報生成手段と、

前記許諾条件を示す情報の認証情報を生成する認証情報生成手段と、

前記認証情報を記憶する記憶手段と

を備えることを特徴とする情報処理装置。

40. 前記記憶手段は、耐タンパー性を有する構造であることを



特徴とする請求の範囲第39項に記載の情報処理装置。

41. 暗号化されている情報を復号して利用する情報処理方法において、

前記情報の使用の許諾条件を示す情報を生成する許諾情報生成ステップと、

前記許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、

前記認証情報を記憶する記憶ステップと

を含むことを特徴とする情報処理方法。

42. 暗号化されている情報を復号して利用する情報処理装置に、

前記情報の使用の許諾条件を示す情報を生成する許諾情報生成ステップと、

前記許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、

前記認証情報を記憶する記憶ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

43. 装着された情報記憶媒体に情報を記憶させて利用する情報処理装置において、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、

前記認証情報を記憶する記憶手段と、

前記関連情報から、他の認証情報を生成し、前記記憶手段が記憶している前記認証情報との一致を検証する検証手段と、

前記情報記憶媒体と相互認証する相互認証手段と

を備えることを特徴とする情報処理装置。

44. 前記情報を暗号化する暗号化手段を更に備えることを特徴とする請求の範囲第43項に記載の情報処理装置。

45. 前記認証情報を暗号化する暗号化手段を更に備えることを特徴とする請求の範囲第43項に記載の情報処理装置。

46. 前記記憶手段が記憶する暗号化されている前記認証情報を復号する復号手段を更に備えることを特徴とする請求の範囲第45項に記載の情報処理装置。

47. 装着された情報記憶媒体に情報を記憶させて利用する情報処理装置の情報処理方法において、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、

前記認証情報を記憶する記憶ステップと、

前記関連情報から、他の認証情報を生成し、前記記憶ステップで記憶した前記認証情報との一致を検証する検証ステップと、

前記情報記憶媒体と相互認証する相互認証ステップと

を含むことを特徴とする情報処理方法。

48. 装着された情報記憶媒体に情報を記憶させて利用する情報処理装置に、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、

前記認証情報を記憶する記憶ステップと、

前記関連情報から、他の認証情報を生成し、前記記憶ステップで記憶した前記認証情報との一致を検証する検証ステップと、

前記情報記憶媒体と相互認証する相互認証ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

49. 暗号化された情報を記憶し、情報処理装置に装着される情報記憶媒体において、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、

前記認証情報を記憶する記憶手段と、

前記関連情報から、他の認証情報を生成し、前記記憶手段が記憶している前記認証情報との一致を検証する検証手段と、

前記情報処理装置と相互認証する相互認証手段と

を備えることを特徴とする情報記憶媒体。

50. 前記認証情報を暗号化する暗号化手段を更に備えることを特徴とする請求の範囲第49項に記載の情報記憶媒体。

51. 前記記憶手段が記憶する暗号化されている前記認証情報を復号する復号手段を更に備えることを特徴とする請求の範囲第49項に記載の情報記憶媒体。

52. 情報提供者に代わり、前記情報提供者が提供する情報の利用者から利用料金を徴収し、情報提供者に利益を分配する情報処理装置において、

前記情報を特定するデータ及び前記情報の利用に対する前記情報提供者への支払金額を示すデータを記憶する記憶手段と、

前記記憶手段が記憶するデータを基に、前記情報提供者毎への支払金額の合計を算出する算出手段と、

前記情報提供者毎の利益を基に、決済機関に対し前記情報提供者毎の決済を指示する決済指示手段と

を備えることを特徴とする情報処理装置。

53. 前記算出手段は、前記情報提供業者間の支払金額の合計をさらに算出することを特徴とする請求の範囲第52項に記載の情報処理装置。

54. 前記記憶手段は、前記情報の著作権を徴収する団体への支払金額に関する情報をさらに記憶し、

前記算出手段は、前記団体への支払金額の合計をさらに算出し、  
前記決済指示手段は、前記決済機関に対し前記団体の決済をさらに指示する

ことを特徴とする請求の範囲第52項に記載の情報処理装置。

55. 前記記憶手段は、情報の利用料金の割引のデータをさらに記憶することを特徴とする請求の範囲第52項に記載の情報処理装置。

56. 前記決済指示手段は、前記情報提供業者毎の決済機関に関する情報を記憶することを特徴とする請求の範囲第52項に記載の情報処理装置。

57. 情報提供業者に代わり、前記情報提供業者が提供する情報の利用者から利用料金を徴収し、情報提供業者に利益を分配する情報処理方法において、

前記情報を特定するデータ及び前記情報の利用に対する前記情報提供業者への支払金額を示すデータを記憶する記憶ステップと、

前記記憶ステップで記憶するデータを基に、前記情報提供業者毎への支払金額の合計を算出する算出ステップと、

前記情報提供業者毎の利益を基に、決済機関に対し前記情報提供業者毎の決済を指示する決済指示ステップと

を含むことを特徴とする情報処理方法。

58. 情報提供業者に代わり、前記情報提供業者が提供する情報の利用者から利用料金を徴収し、情報提供業者に利益を分配する情報処理装置に、

前記情報を特定するデータ及び前記情報の利用に対する前記情報提供業者への支払金額を示すデータを記憶する記憶ステップと、

前記記憶ステップで記憶するデータを基に、前記情報提供業者毎への支払金額の合計を算出する算出ステップと、

前記情報提供業者毎の利益を基に、決済機関に対し前記情報提供業者毎の決済を指示する決済指示ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

59. 装着された外部記憶媒体に所定の情報を記憶させるとともに、暗号化された情報を復号し、利用する情報処理装置において、

装着された前記外部記憶媒体と相互認証する相互認証手段と、

所定の鍵で所定の情報を暗号化する暗号化手段と

を備えることを特徴とする情報処理装置。

60. 前記所定の鍵は、前記情報処理装置を管理する管理装置の公開鍵であることを特徴とする請求の範囲第59項に記載の情報処理装置。

61. 装着された外部記憶媒体に所定の情報を記憶させるとともに、暗号化された情報を復号し、利用する情報処理装置の情報処理方法において、

装着された前記外部記憶媒体と相互認証する相互認証ステップと、

所定の鍵で所定の情報を暗号化する暗号化ステップと

を含むことを特徴とする情報処理方法。

6 2. 装着された外部記憶媒体に所定の情報を記憶させるとともに、暗号化された情報を復号し、利用する情報処理装置に、装着された前記外部記憶媒体と相互認証する相互認証ステップと、所定の鍵で所定の情報を暗号化する暗号化ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

6 3. 暗号化された情報を復号し、利用する情報処理装置を管理する管理装置において、

前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号手段を備えることを特徴とする管理装置。

6 4. 暗号化された情報を復号し、利用する情報処理装置を管理する管理方法において、

前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップを含むことを特徴とする管理方法。

6 5. 暗号化された情報を復号し、利用する情報処理装置を管理する管理装置に、

前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップ

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

6 6. 装着された外部記憶媒体に所定の情報を記憶させるとともに、暗号化された情報を復号し、利用する情報処理装置及び前記情報処理装置を管理する管理装置からなる情報利用システムにおいて、

前記情報処理装置は、装着された前記外部記憶媒体と相互認証す

る相互認証手段と、前記管理装置の公開鍵で所定の情報を暗号化する暗号化手段とを備え、

前記管理装置は、前記外部記憶媒体に記憶されたデータを復号する復号手段を備える

ことを特徴とする情報利用システム。

67. 暗号化された情報を復号し、利用する情報処理装置に装着される外部記憶媒体において、

前記情報処理装置と相互認証する相互認証手段を備えることを特徴とする外部記憶媒体。

**THIS PAGE BLANK (USPTO)**

---



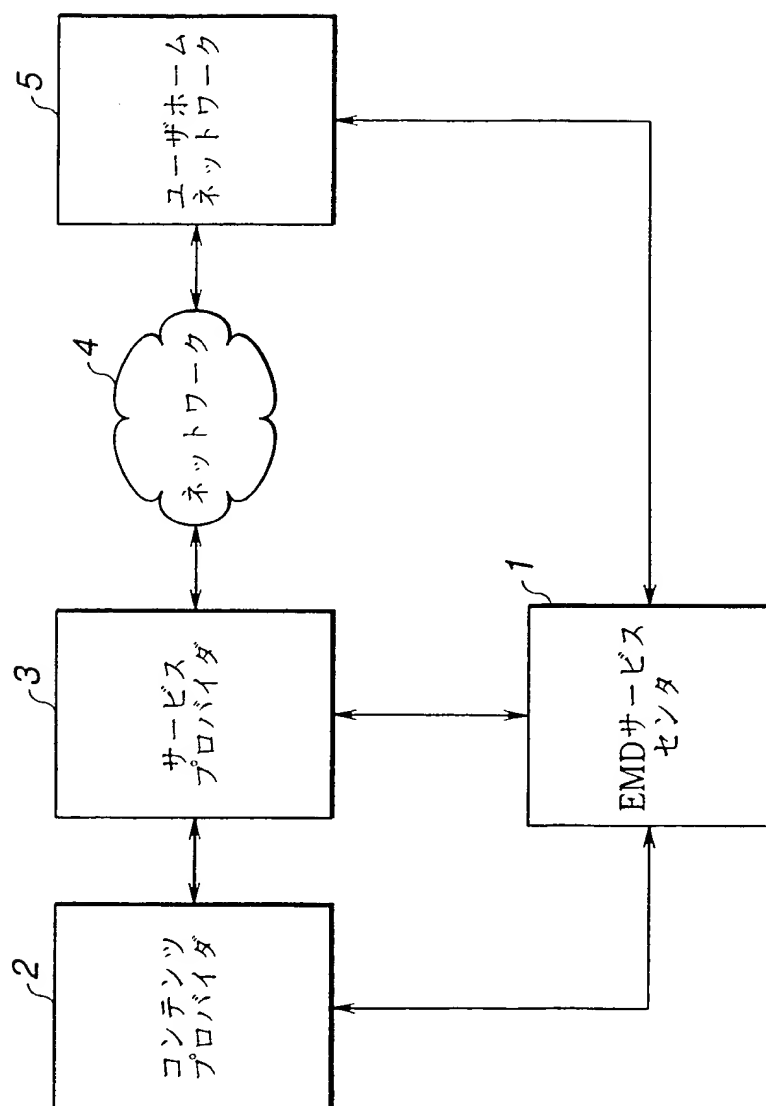


FIG.1

**THIS PAGE BLANK (USPTO)**

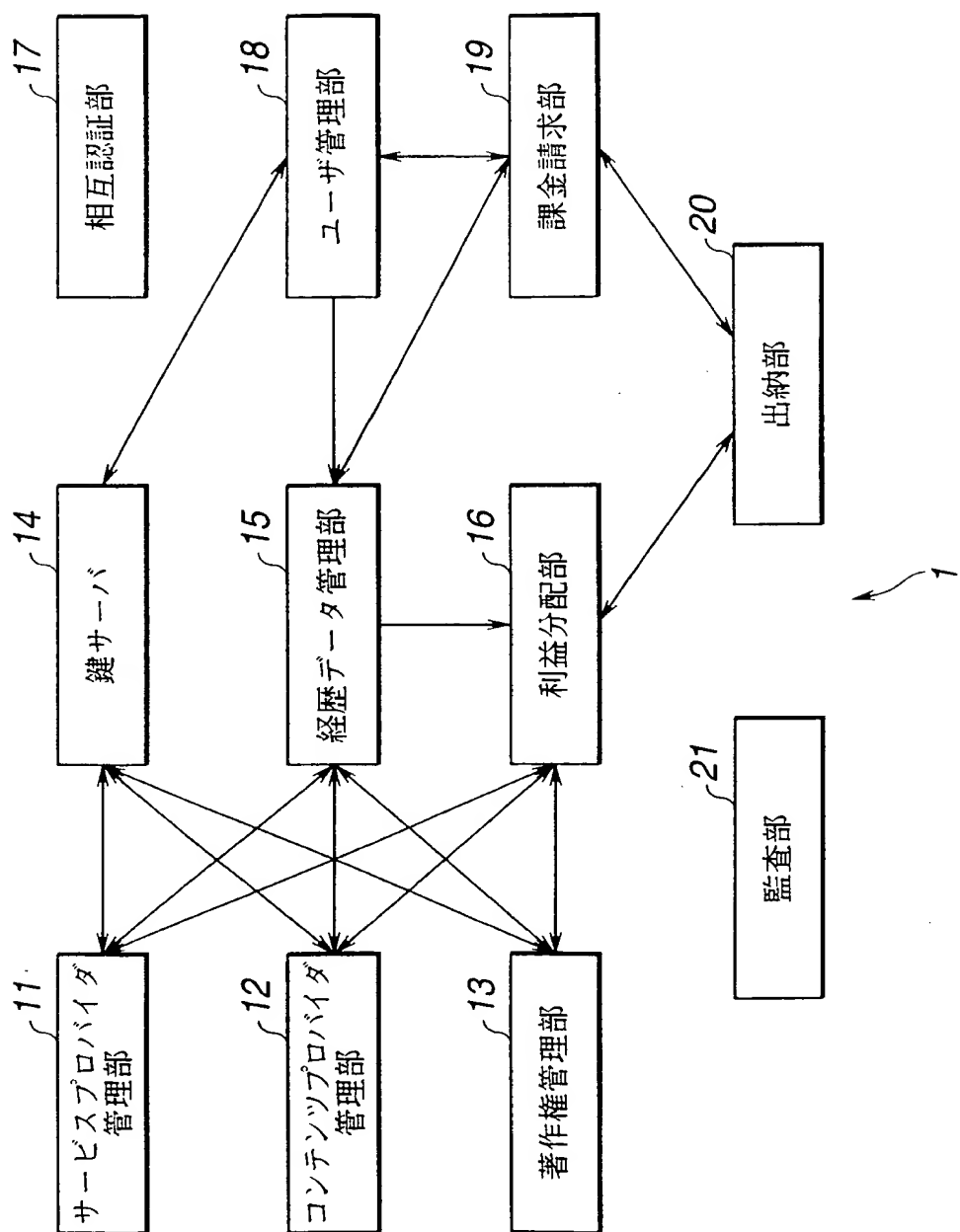


FIG.2

**THIS PAGE BLANK (USPTO)**

---

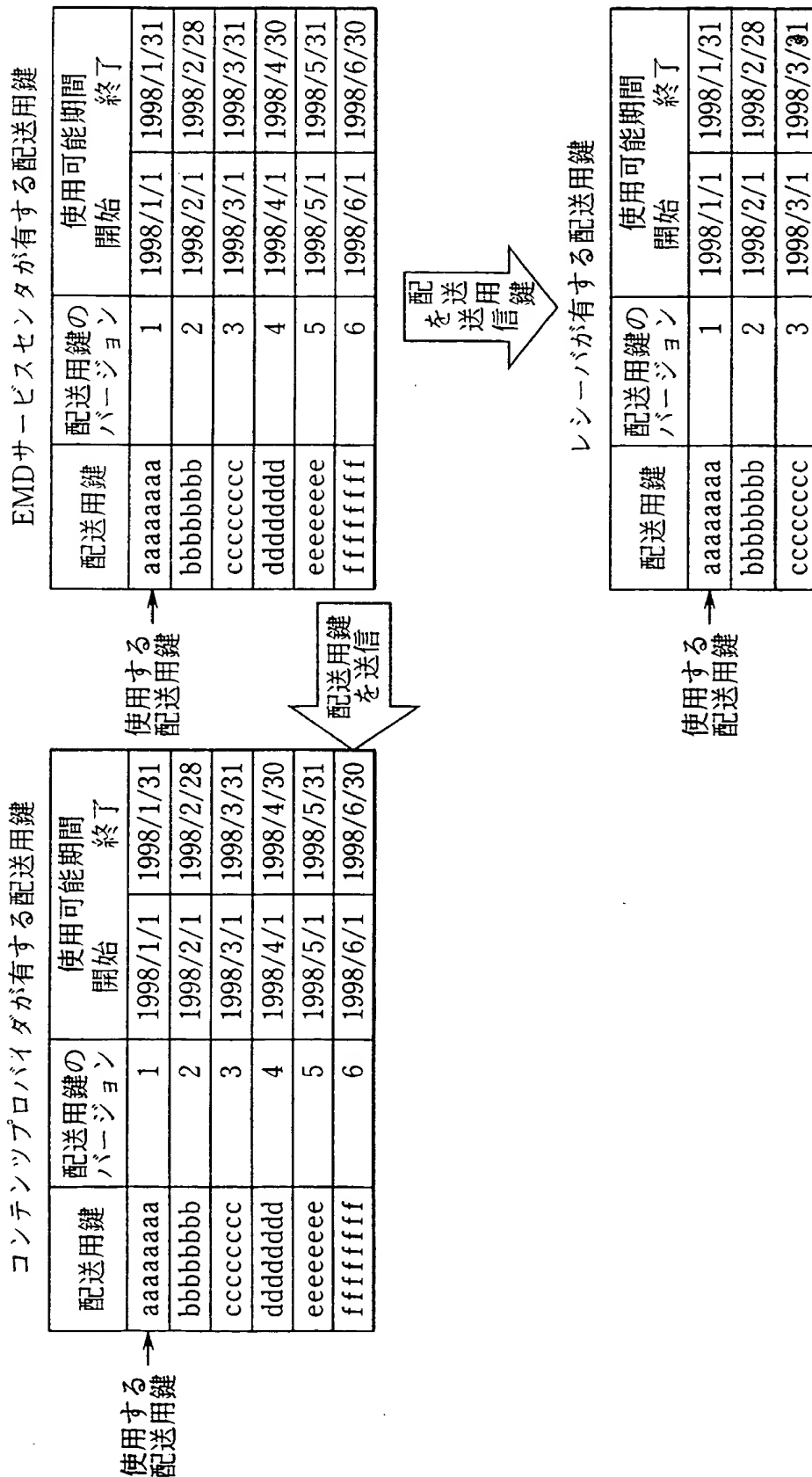


FIG.3

**THIS PAGE BLANK (USPTO)**

---

4/88

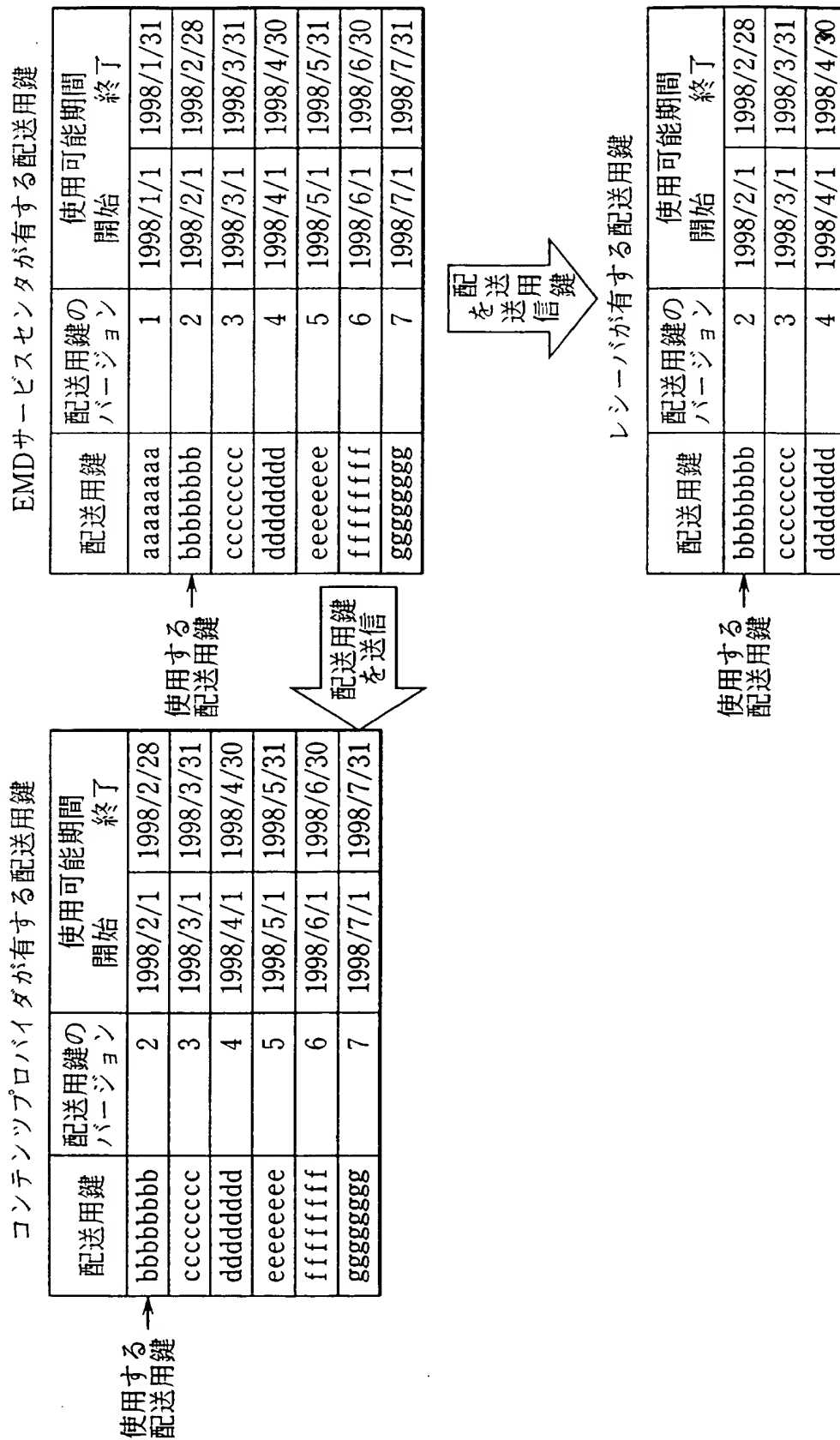


FIG.4

**THIS PAGE BLANK (USPTO)**

---



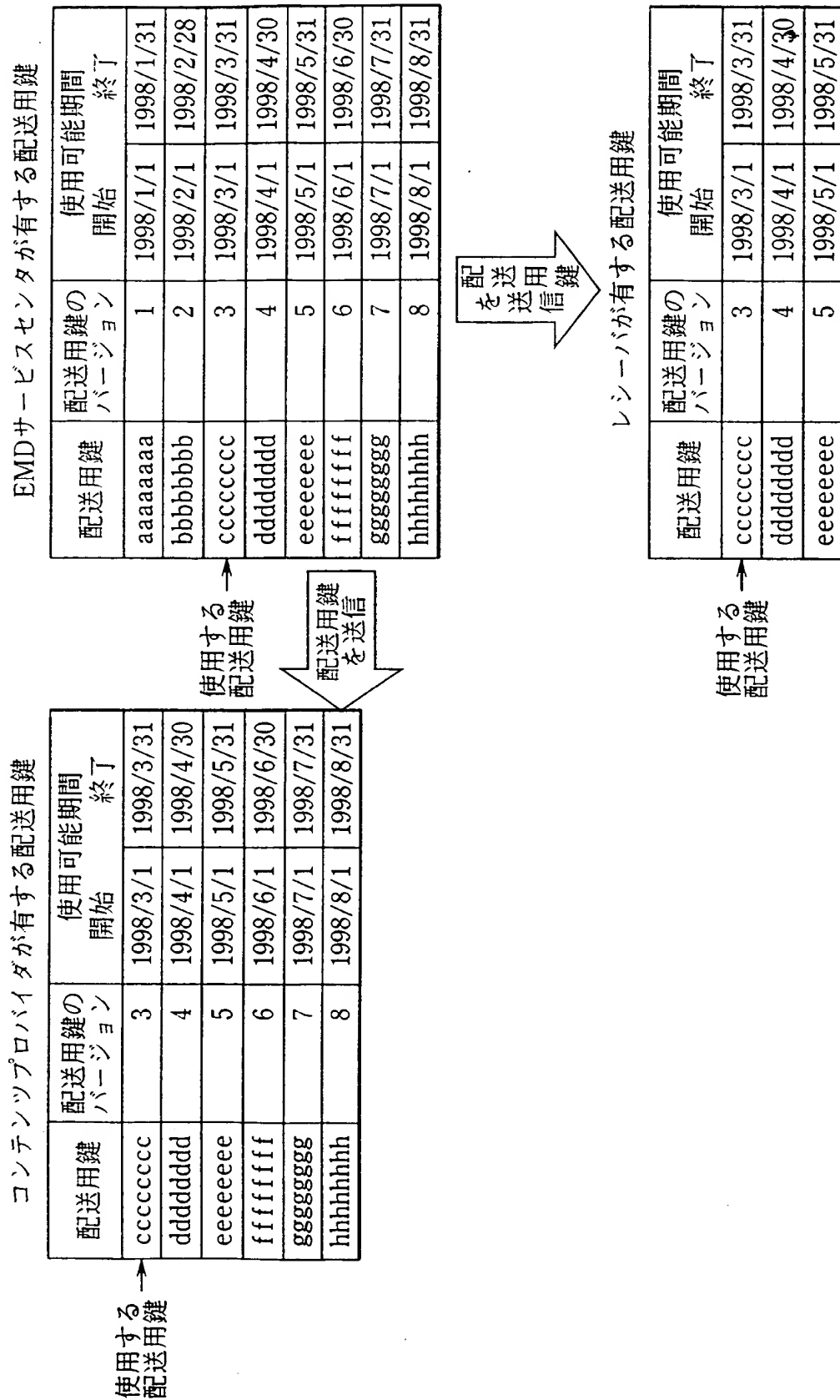


FIG.5

**THIS PAGE BLANK (USPTO)**

---

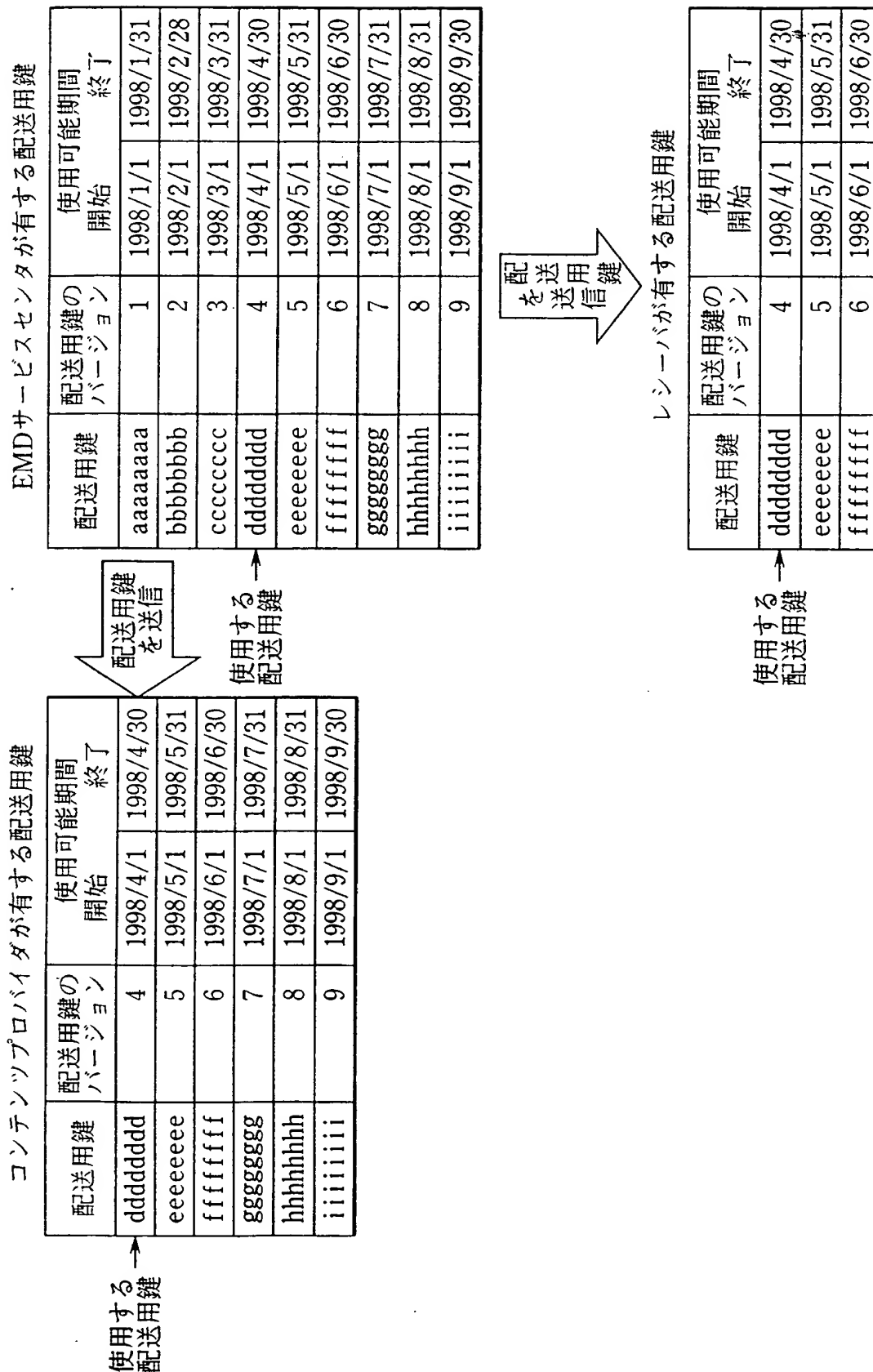


FIG.6

**THIS PAGE BLANK (USPTO)**

7/88

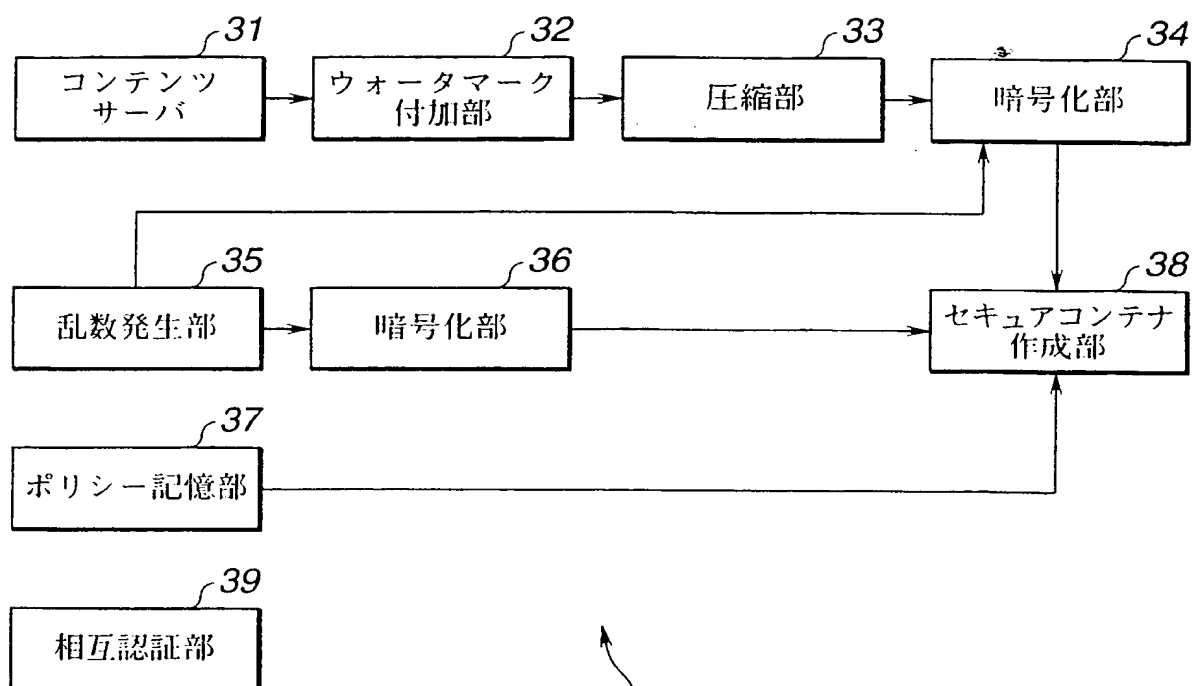
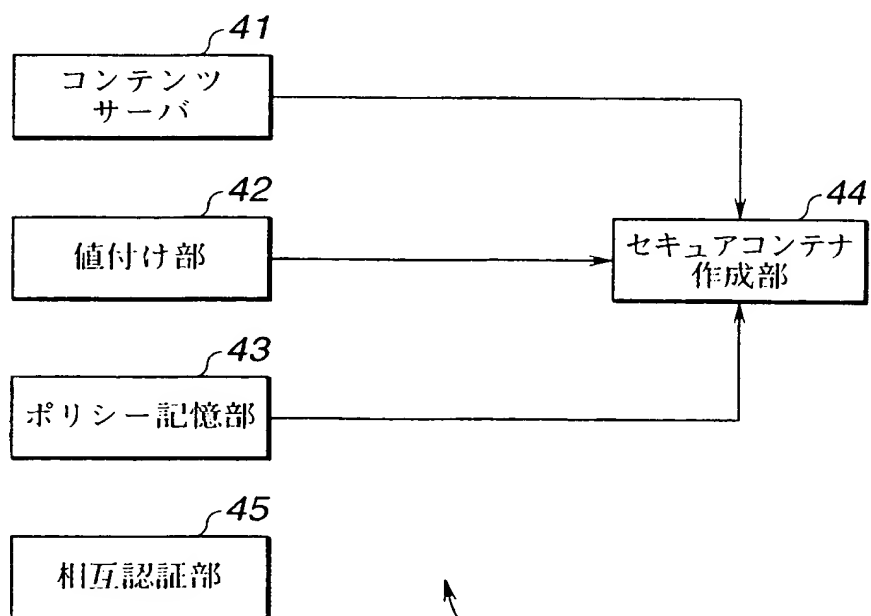
ID	決済処理	登録	EMDサービスセンタとの接続
000000000000000001h	可	可	可
000000000000000002h	可	可	不可
000000000000000003h	可	不可	可
000000000000000004h	可	不可	不可
000000000000000005h	不可	可	可
000000000000000006h	不可	可	不可
000000000000000007h	不可	不可	可
000000000000000008h	不可	不可	不可
000000000000000009h	可	可	可
. . .			
FFFFFFFFFFFFFFFFFEh	可	不可	不可
FFFFFFFFFFFFFFFFFh	不可	可	可

FIG.7

**THIS PAGE BLANK (USPTO)**

---

8/88

2  
**FIG. 8**3  
**FIG. 9**

**THIS PAGE BLANK (USPTO)**



9/88

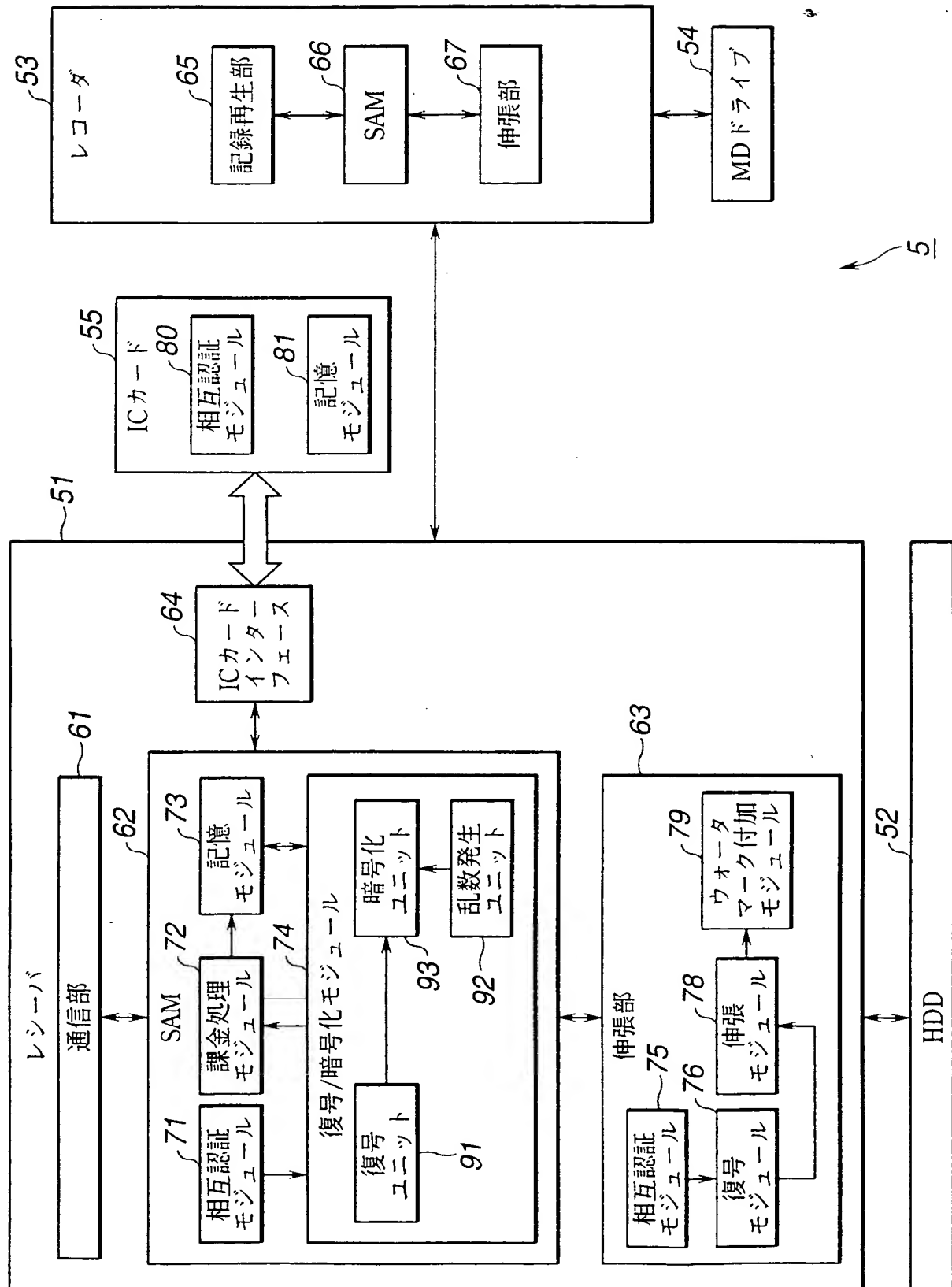


FIG.10

**THIS PAGE BLANK (USPTO)**

10/88

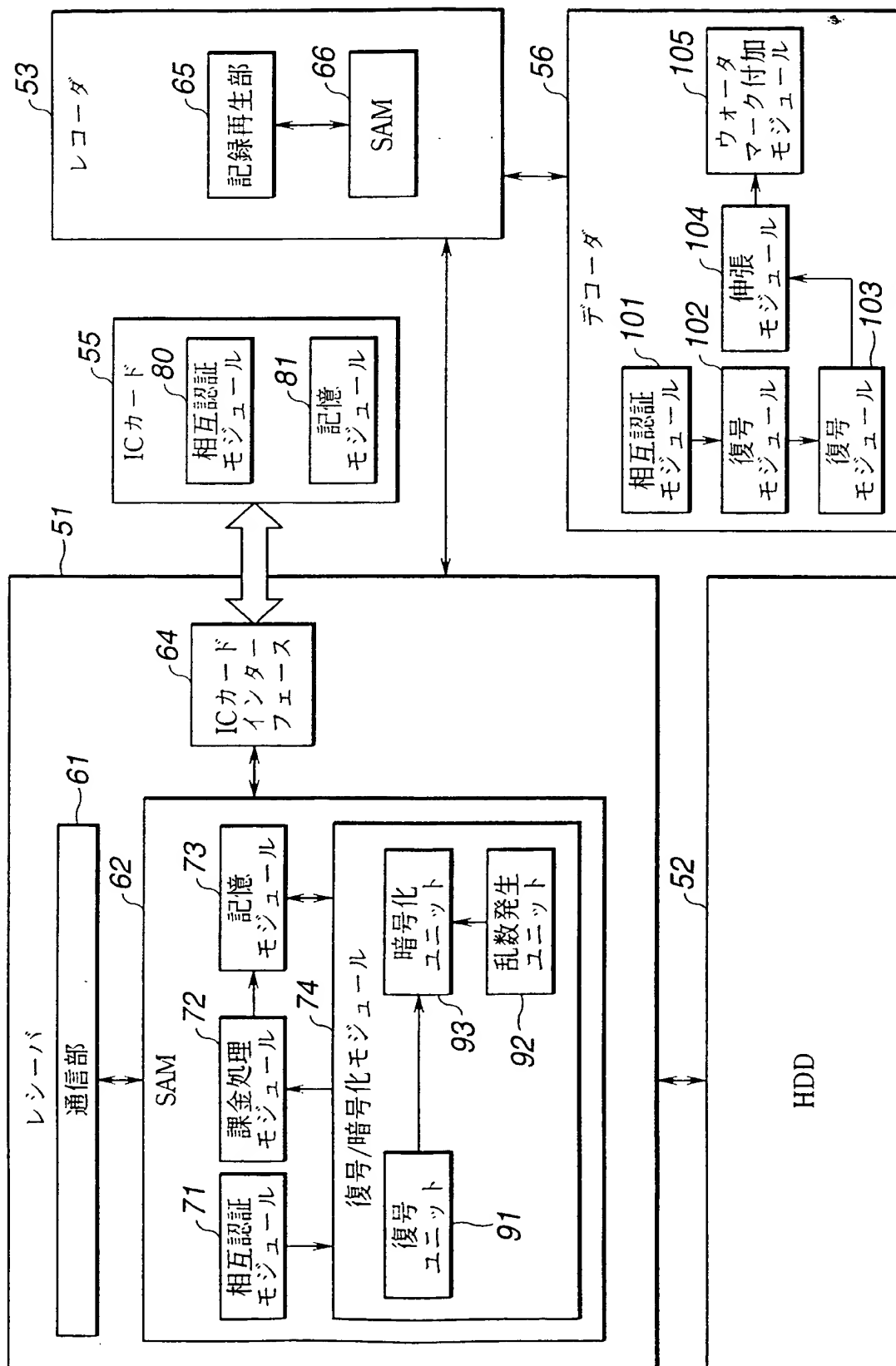


FIG.11

**THIS PAGE BLANK (USPTO)**

---

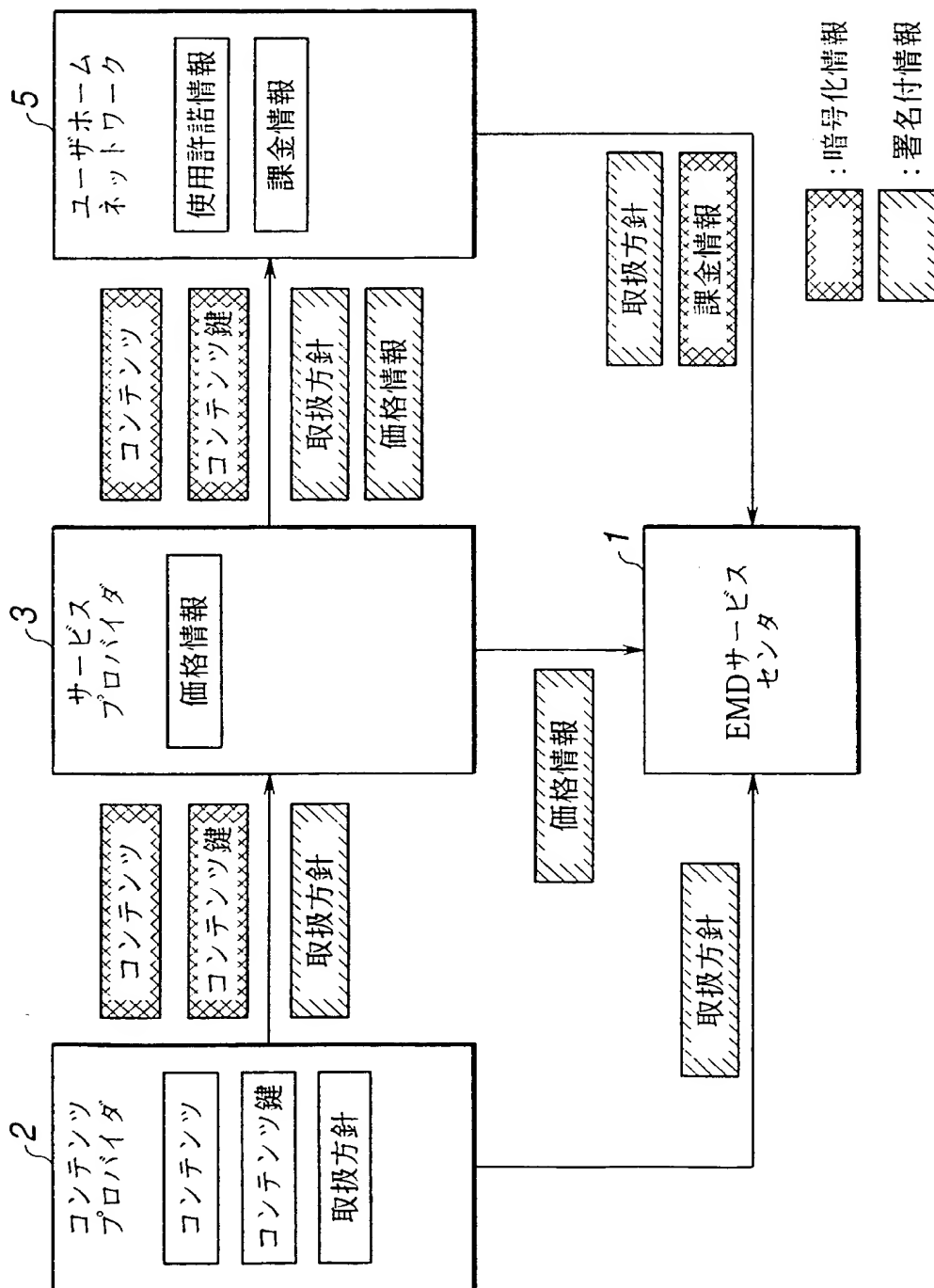


FIG.12

**THIS PAGE BLANK (USPTO)**

---

12/88

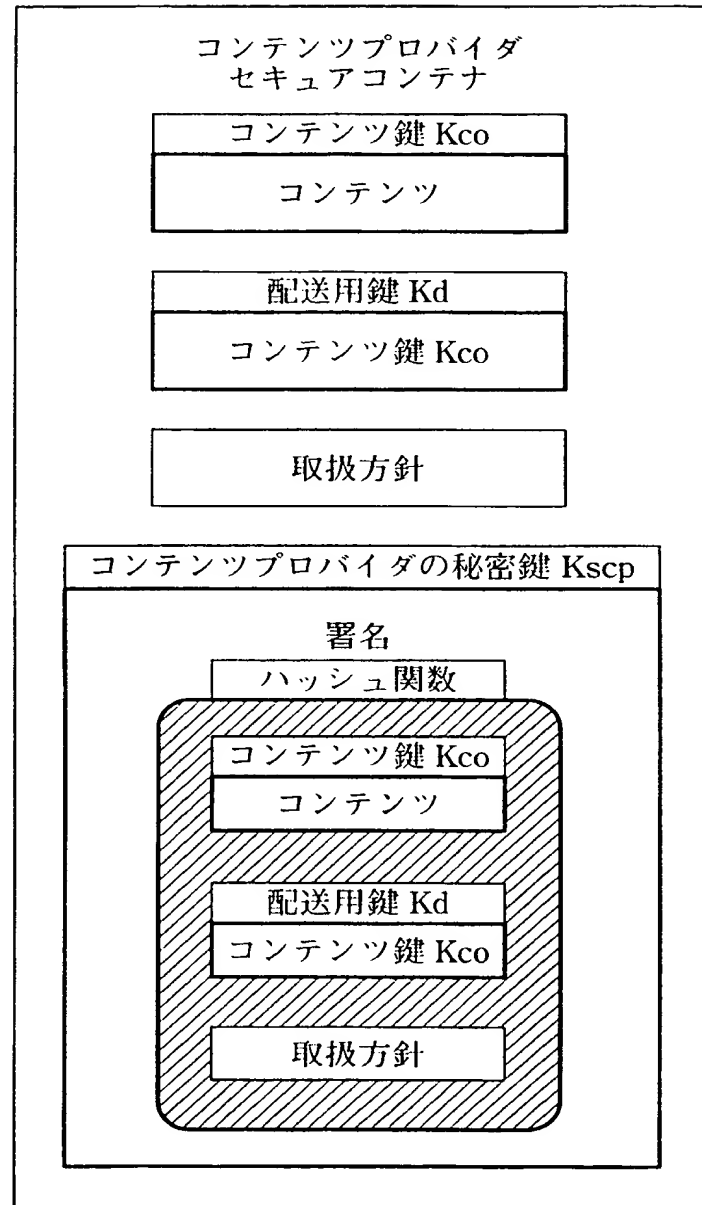


FIG.13

**THIS PAGE BLANK (USPTO)**

---



13/88



FIG.14

**THIS PAGE BLANK (USPTO)**

---

14/88

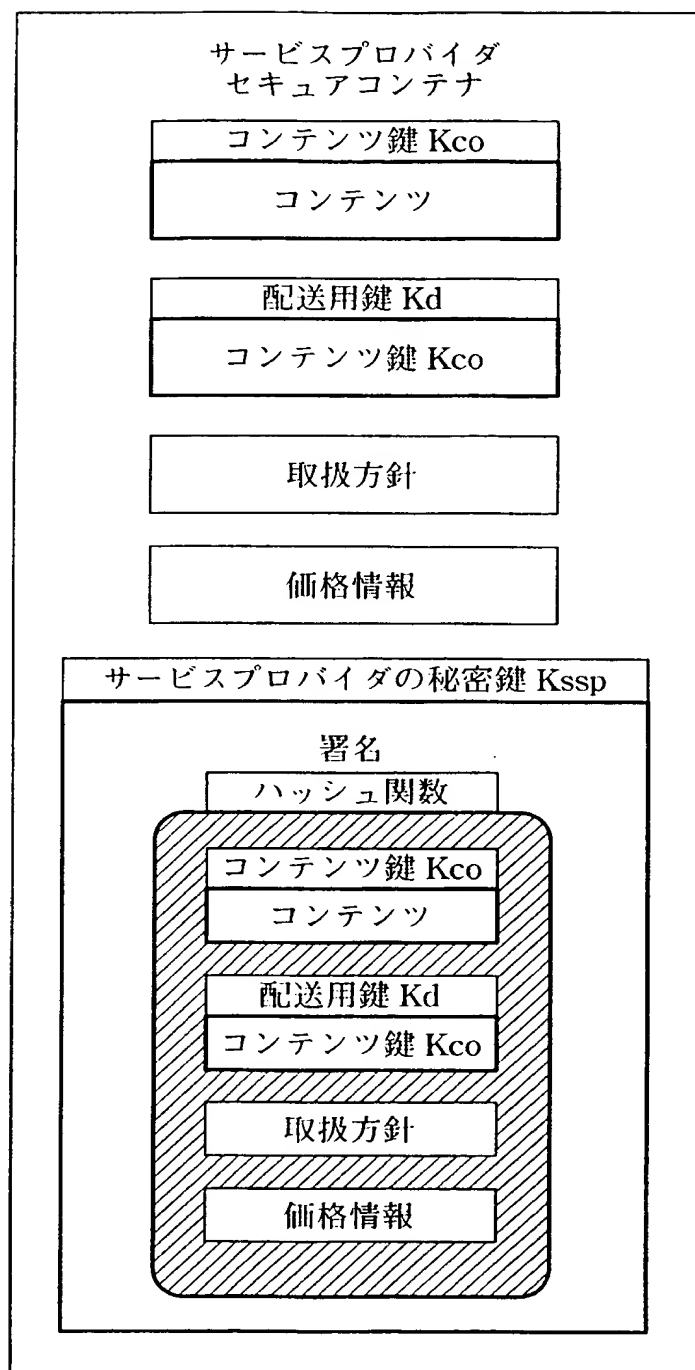


FIG.15

**THIS PAGE BLANK (USPTO)**

---

15/88

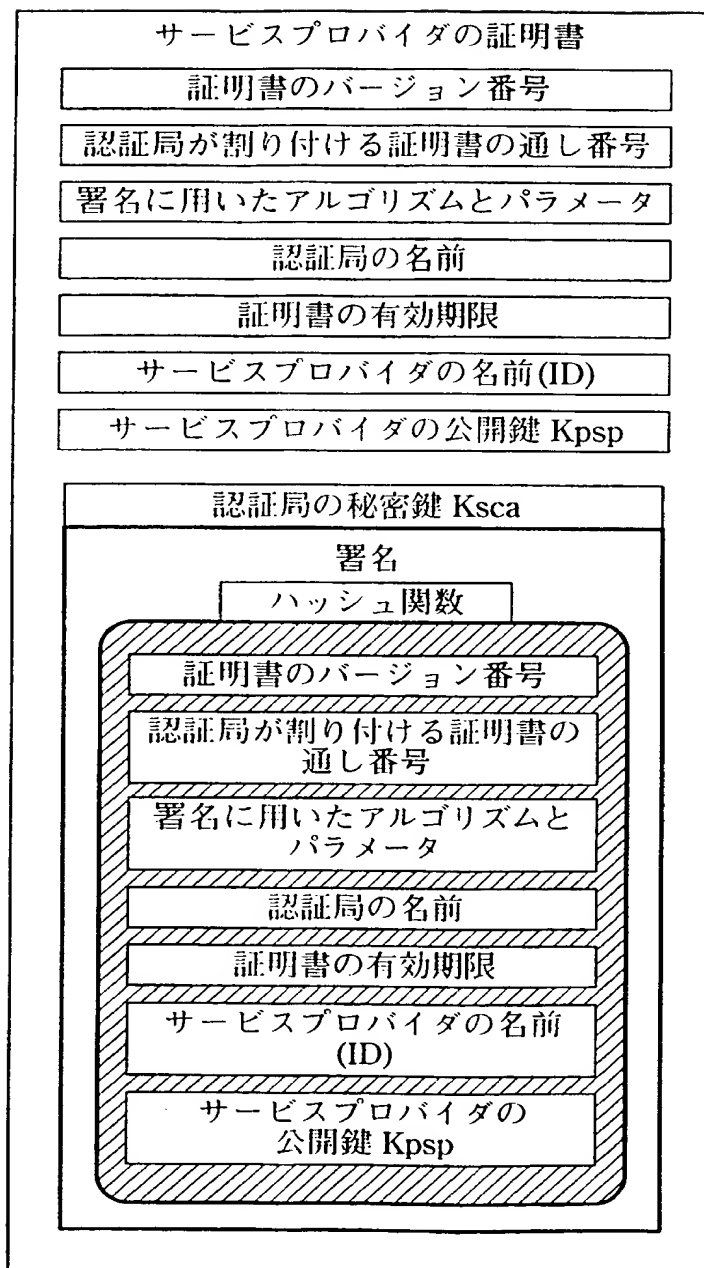


FIG.16

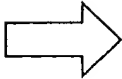
**THIS PAGE BLANK (USPTO)**

---

利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1

取扱方針

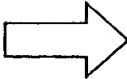
FIG.17A



利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
価格	150円	-	80円

取扱方針  
及び  
価格情報

FIG.17B



利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	0

使用許諾  
情報

FIG.17C

**THIS PAGE BLANK (USPTO)**



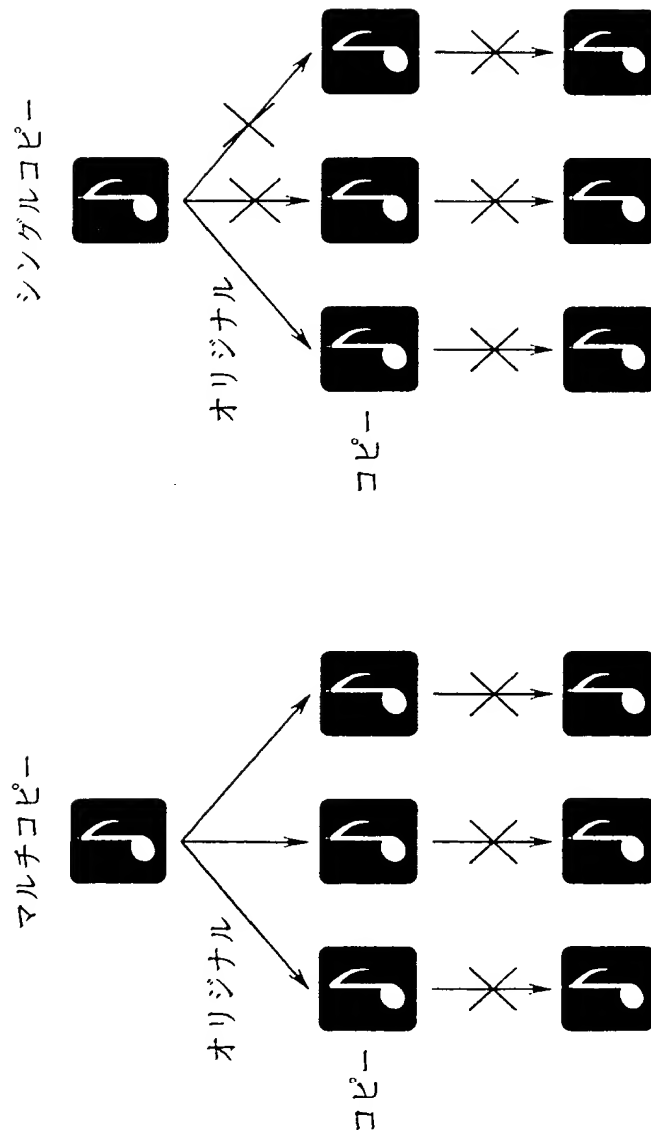


FIG.18A

FIG.18B

**THIS PAGE BLANK (USPTO)**

---

FIG.19A

取扱方針  
及び  
利益分配

利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
利益分配	70円	.	40円

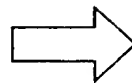


FIG.19B

取扱方針  
利益分配  
及び  
価格情報

利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
利益分配	60円	.	30円
分配価格	150円	.	80円

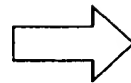


FIG.19C

課金情報

利用内容	再生	シングルコピー	マルチコピー
利用回数	1	0	0

**THIS PAGE BLANK (USPTO)**

FIG.20A

取扱方針  
及び  
価格情報

利用内容	再生		
	制限なし	回数制限	期日制限
	—	5	1998/12/31
価格	—	60円	90円

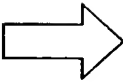


FIG.20B

使用許諾  
情報

利用内容	再生		
	制限なし	回数制限	期日制限
	—	5	—

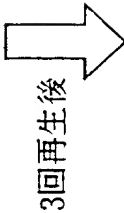


FIG.20C

使用許諾  
情報

利用内容	再生		
	制限なし	回数制限	期日制限
	—	2	—

**THIS PAGE BLANK (USPTO)**

20/88

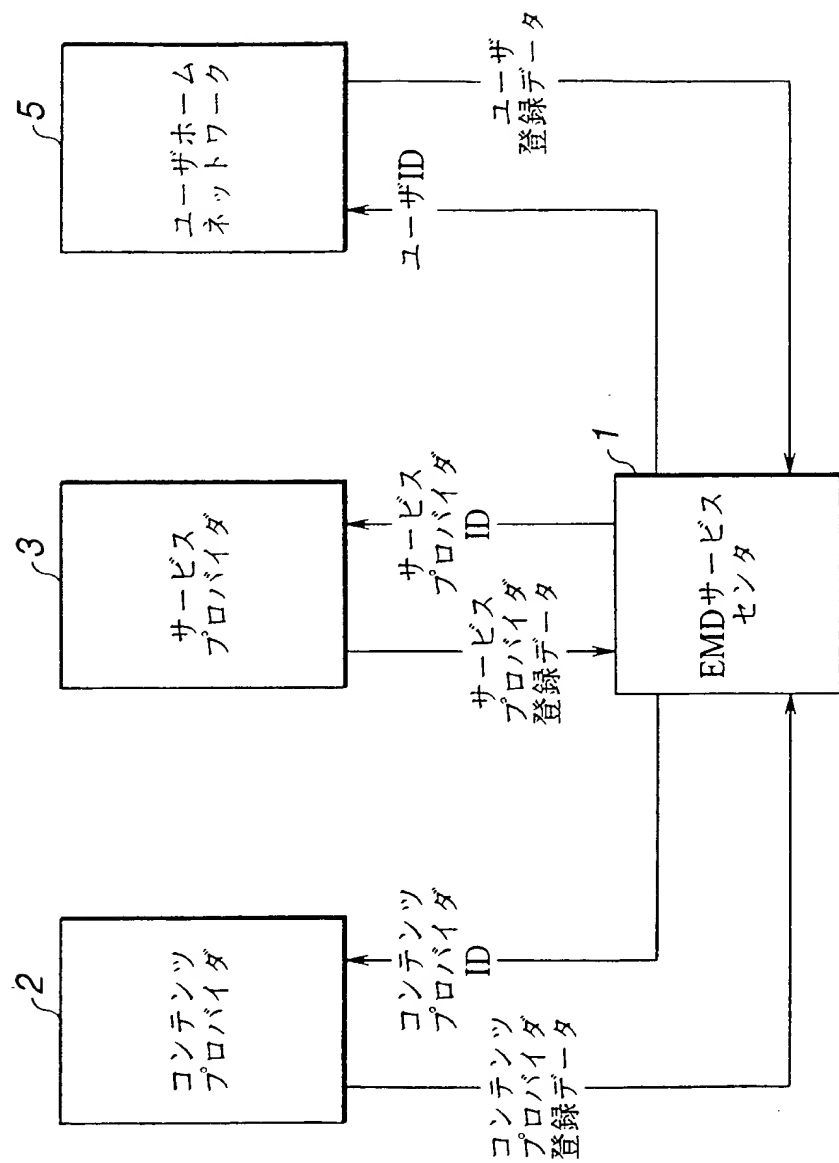


FIG.21

**THIS PAGE BLANK (USPTO)**

---



21/88

コンテンツ ID	コンテンツプロバイダ ID	権利団体
1	201	10%
2	201	20%

FIG.22

**THIS PAGE BLANK (USPTL)**

プロバイダ ID	コンテンツ ID	割引率	期間
コンテンツツプロバイダ 1	1	2%	1998.9～1998.12
	2	3%	
	すべてのコンテンツ	1%	
コンテンツツプロバイダ 2	3	5%	
サービスプロバイダ 1	1	3%	
サービスプロバイダ 2	4	1%	

FIG.23

**THIS PAGE BLANK (USPTO,**

23/88

月額固定額	変動額		
1000円	期間	1998.8～1998.9	-10%
	利用料	3000円以上	-5%

FIG.24

**THIS PAGE BLANK (USPTO)**

24/88

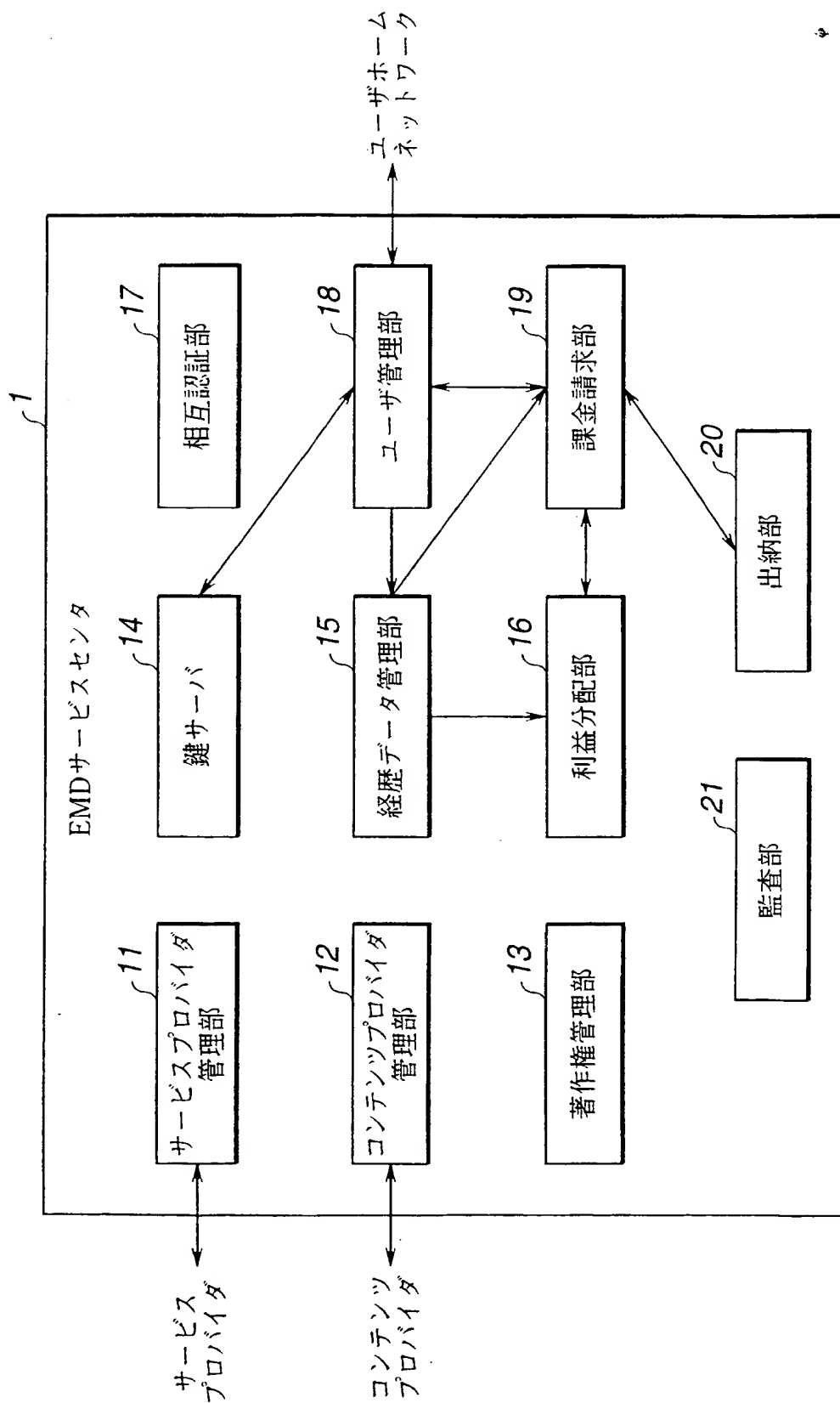


FIG.25

**THIS PAGE BLANK (USPTO)**



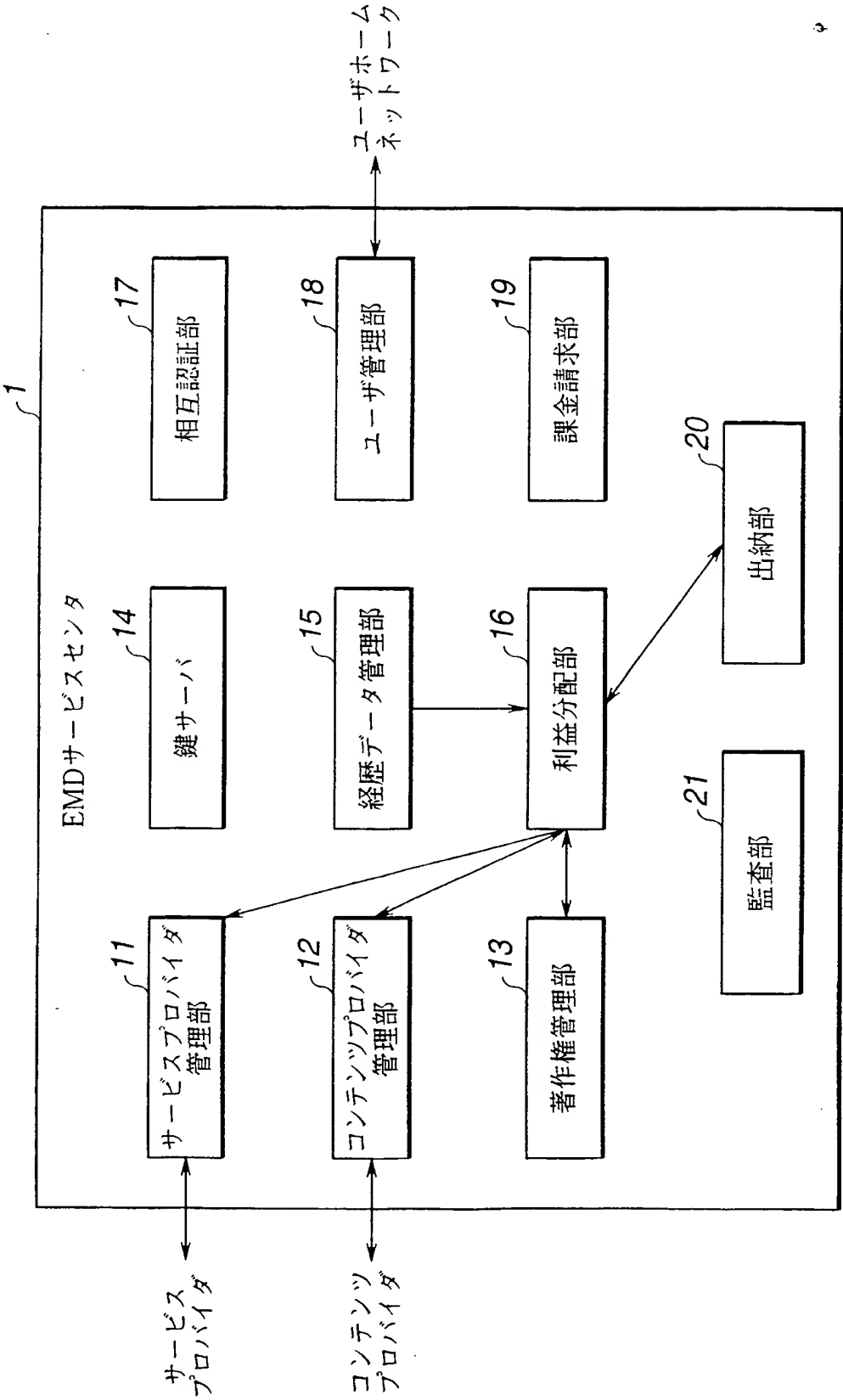


FIG.26

**THIS PAGE BLANK** (USF)

26/88

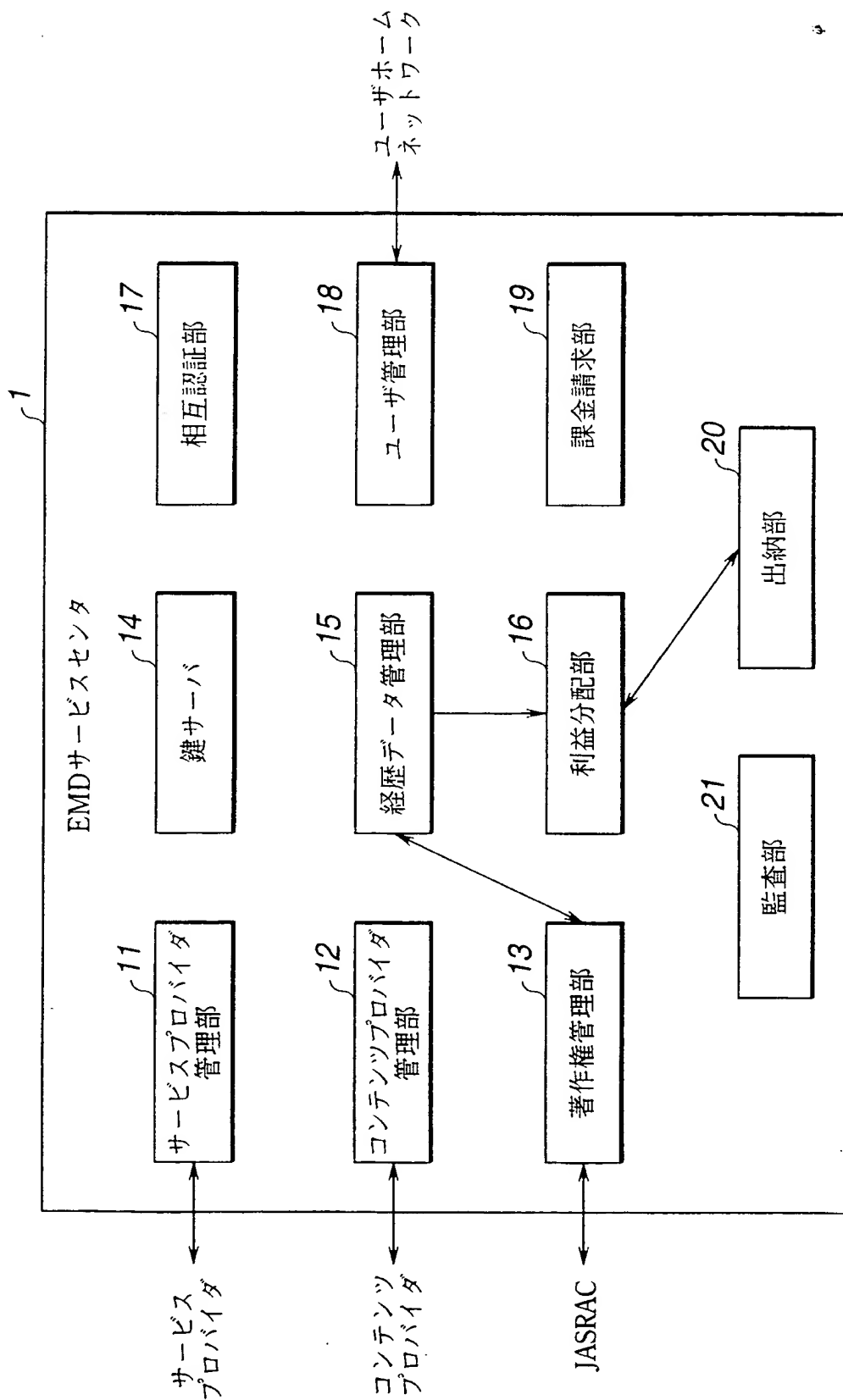


FIG.27

**THIS PAGE BLANK (USPTO)**

---

27/88

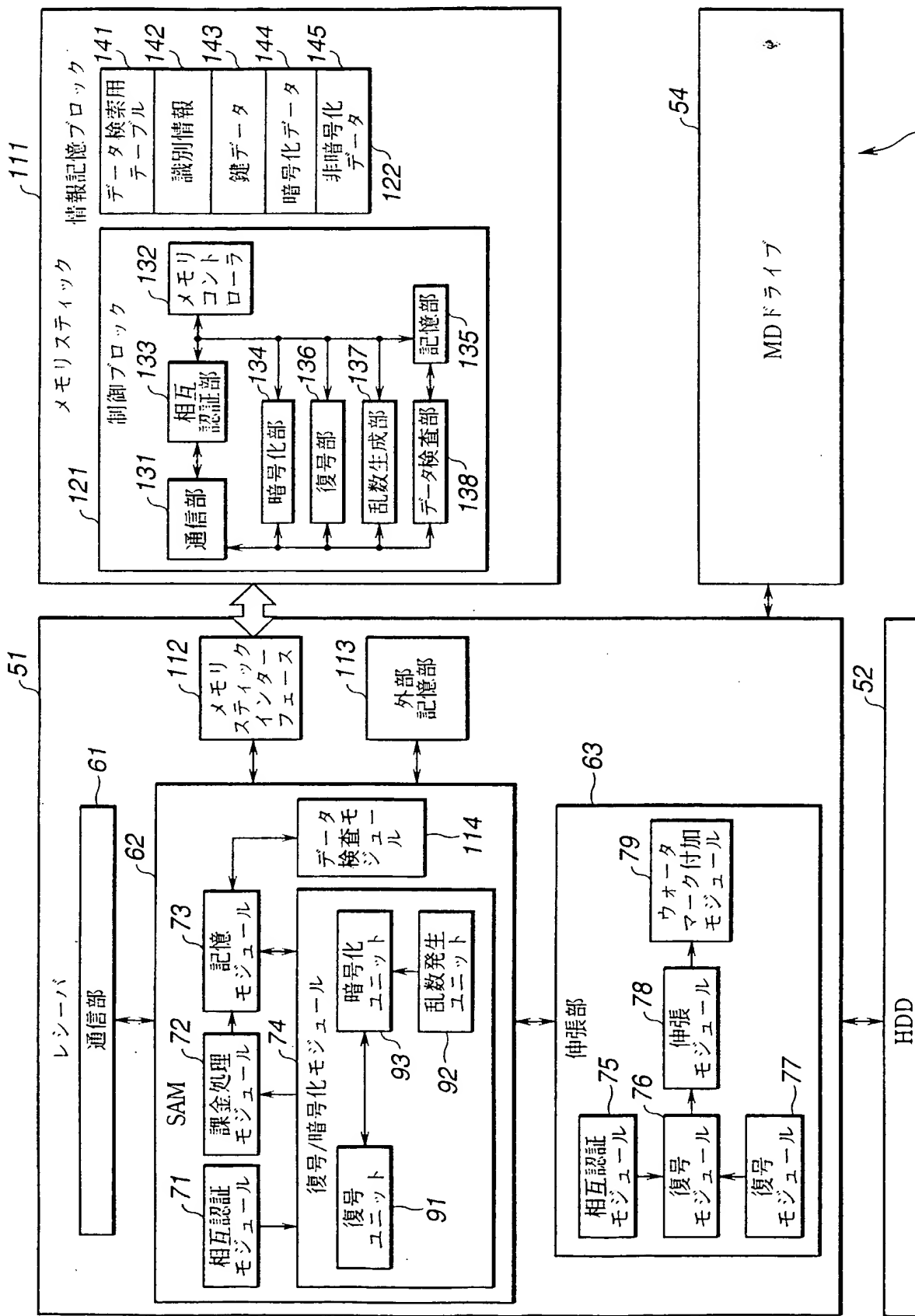


FIG.28

**THIS PAGE BLANK (USPTO,**

鍵データベース1	コンテンツ鍵1	コンテンツID1	使用許諾情報1	コンテンツ鍵2	コンテンツID2	使用許諾情報2
鍵データベース2	コンテンツ鍵3	コンテンツID3	使用許諾情報3	コンテンツ鍵4	コンテンツID4	使用許諾情報4
鍵データベース3	コンテンツ鍵5	コンテンツID5	使用許諾情報5			
鍵データベース4				コンテンツ鍵6	コンテンツID6	使用許諾情報6
鍵データベース5						

FIG.29

**THIS PAGE BLANK (USPTO)**



29/88

秘密鍵				
課金情報				
保存用鍵				
配送用鍵				
...				
検査値 1	検査値 2	検査値 3	検査値 4	検査値 5

FIG.30

**THIS PAGE BLANK (USPT)**

---

30/88

鍵データブロック 1	コンテンツ鍵 1	コンテンツID 1	使用許諾情報 1	コンテンツ鍵 2	コンテンツID 2	使用許諾情報 2
鍵データブロック 2	コンテンツ鍵 3	コンテンツID 3	使用許諾情報 3	コンテンツ鍵 4	コンテンツID 4	使用許諾情報 4
鍵データブロック 3	コンテンツ鍵 5	コンテンツID 5	使用許諾情報 5			
鍵データブロック 4				コンテンツ鍵 6	コンテンツID 6	使用許諾情報 6
鍵データブロック 5						
	検査値 1	検査値 2	検査値 3	検査値 4	検査値 5	

FIG.31

**THIS PAGE BLANK (USPTO)**

秘密鍵
課金情報
保存用鍵
配送用鍵
検査用鍵
...

FIG.32

**THIS PAGE BLANK** (USPTO,

キーデータブロック 1	コンテンツ鍵 1	コンテンツID 1	使用許諾情報 1	コンテンツ鍵 2	コンテンツID 2	使用許諾情報 2
キーデータブロック 2	コンテンツ鍵 3	コンテンツID 3	使用許諾情報 3	コンテンツ鍵 4	コンテンツID 4	使用許諾情報 4
キーデータブロック 3	コンテンツ鍵 5	コンテンツID 5	使用許諾情報 5			
キーデータブロック 4	コンテンツ鍵 6	コンテンツID 6	使用許諾情報 6			

FIG.33

**THIS PAGE BLANK (USPTO)**



33/88

秘密鍵			
保存用鍵			
...			
検査値 1	検査値 2	検査値 3	検査値 4

FIG.34

**THIS PAGE BLANK (USPTO)**

鍵データブロック 1	コンテンツ鍵 1	コンテンツID 1	使用許諾情報 1	コンテンツ鍵 2	コンテンツID 2	使用許諾情報 2
鍵データブロック 2	コンテンツ鍵 3	コンテンツID 3	使用許諾情報 3	コンテンツ鍵 4	コンテンツID 4	使用許諾情報 4
鍵データブロック 3	コンテンツ鍵 5	コンテンツID 5	使用許諾情報 5			
鍵データブロック 4	コンテンツ鍵 6	コンテンツID 6	使用許諾情報 6			
検査値 1			検査値 2	検査値 3	検査値 4	

FIG.35

**THIS PAGE BLANK (USPTO)**

35/88

秘密鍵
検査用鍵
保存用鍵
...

FIG.36

**THIS PAGE BLANK (USPTO)**

36/88

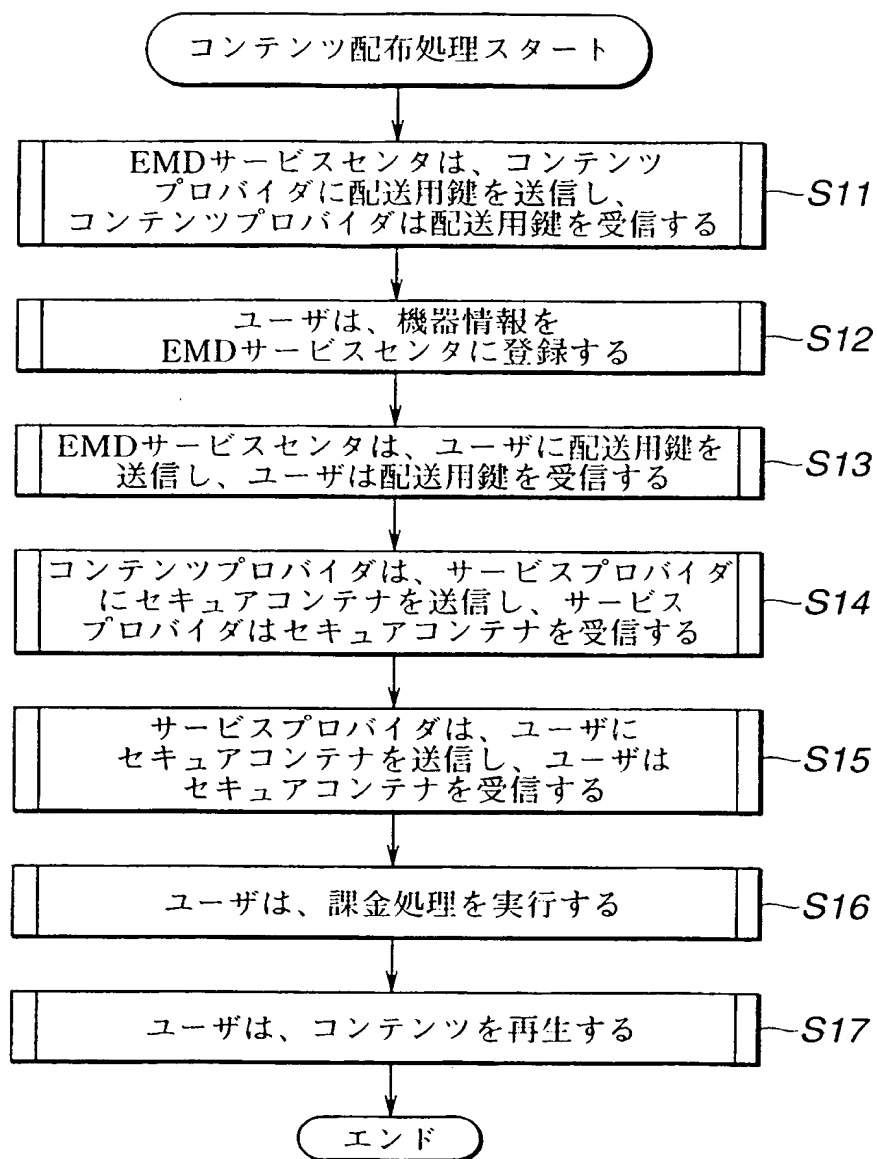


FIG.37

**THIS PAGE BLANK (USPTO)**



37/88

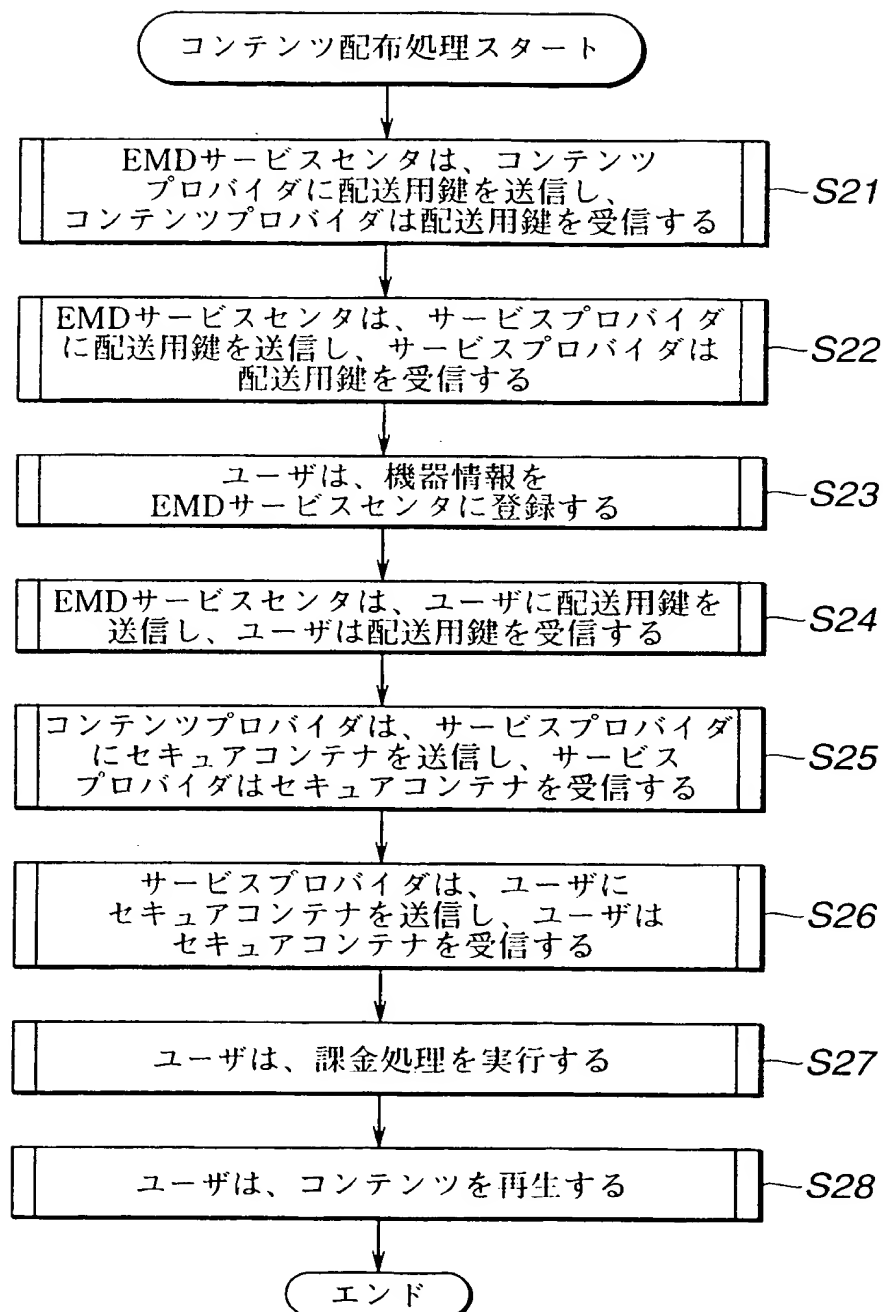


FIG.38

**THIS PAGE BLANK (USPTO)**

38/88

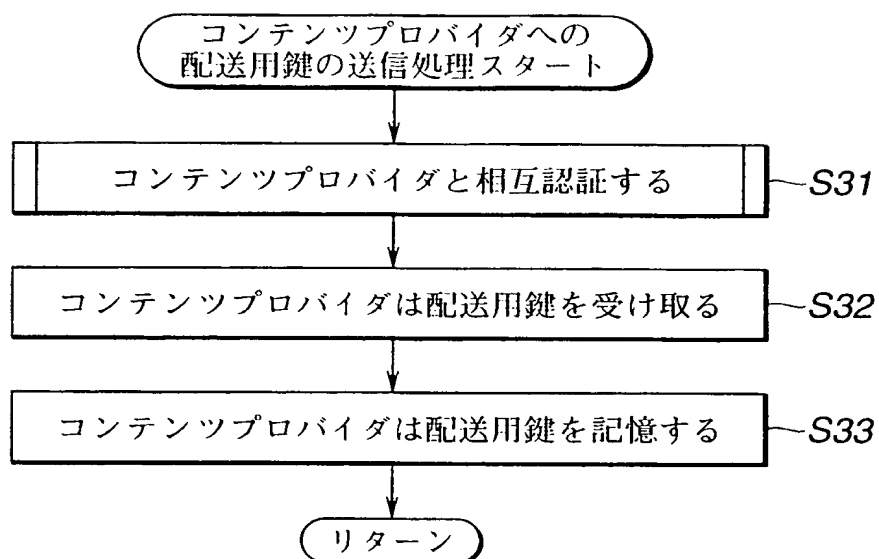


FIG.39

**THIS PAGE BLANK (USPTO)**

---

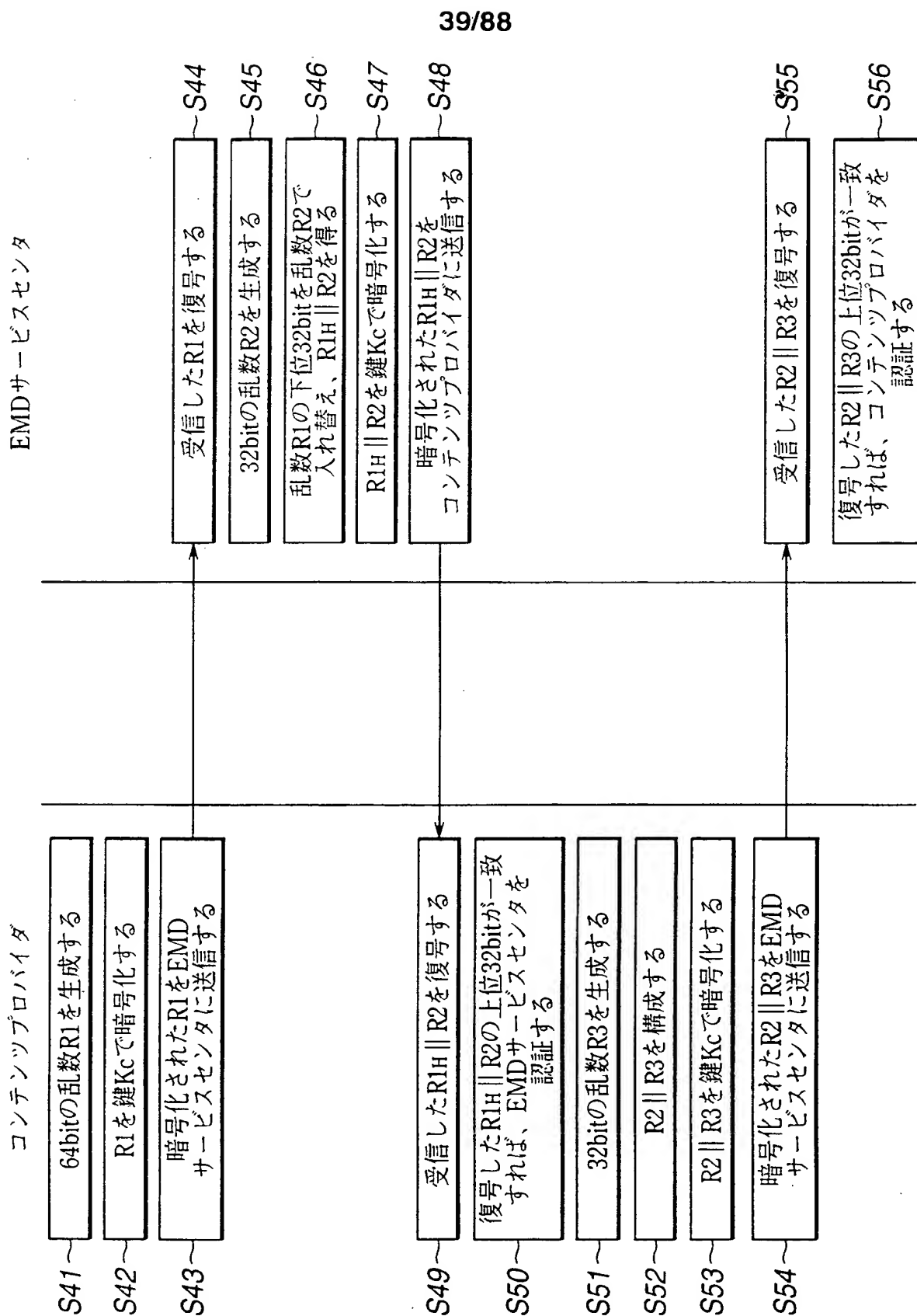


FIG.40

**THIS PAGE BLANK (USPTO)**

40/88

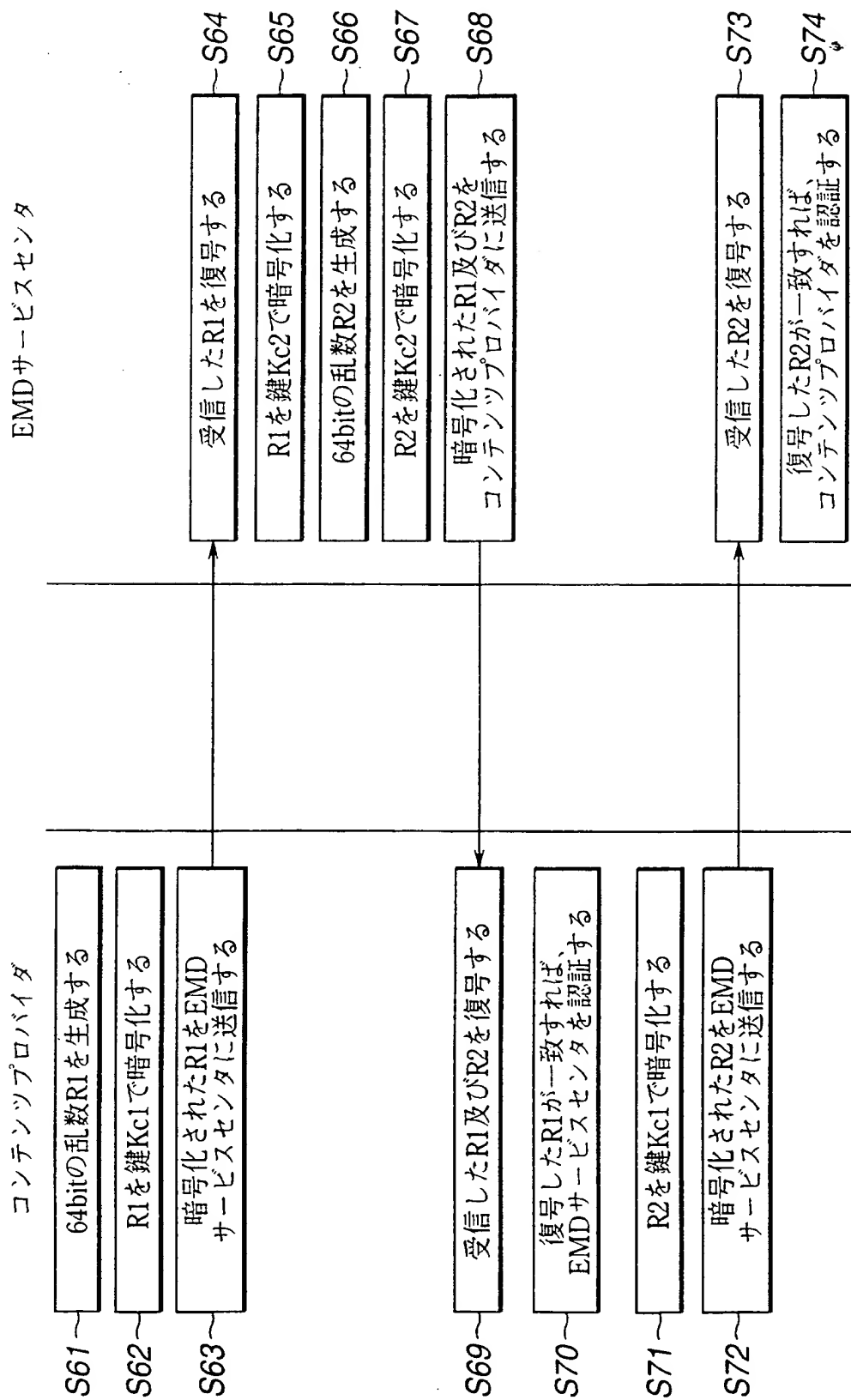


FIG.41

**THIS PAGE BLANK (USPTO)**



41/88

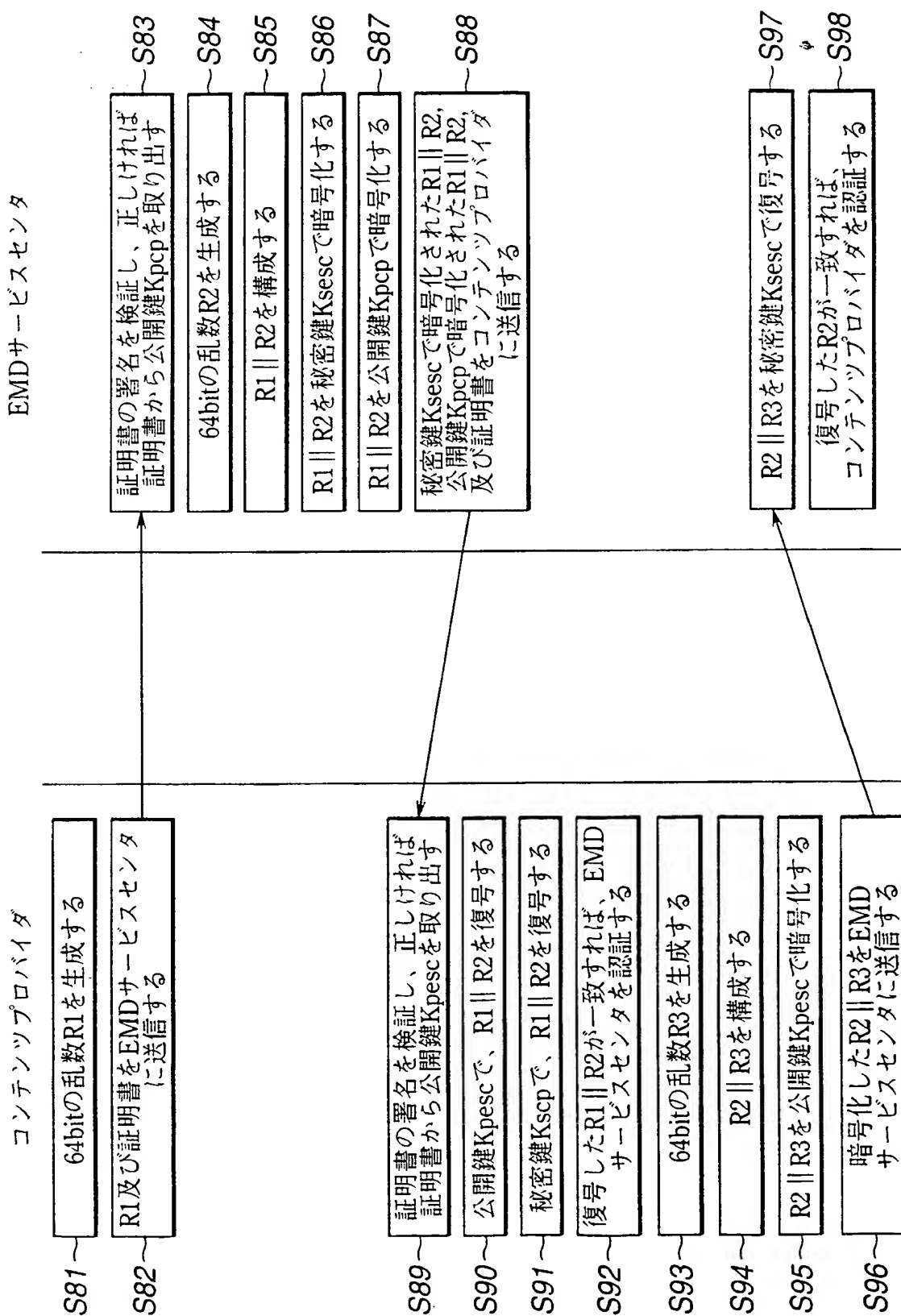


FIG.42

**THIS PAGE BLANK (USPTO)**

42/88

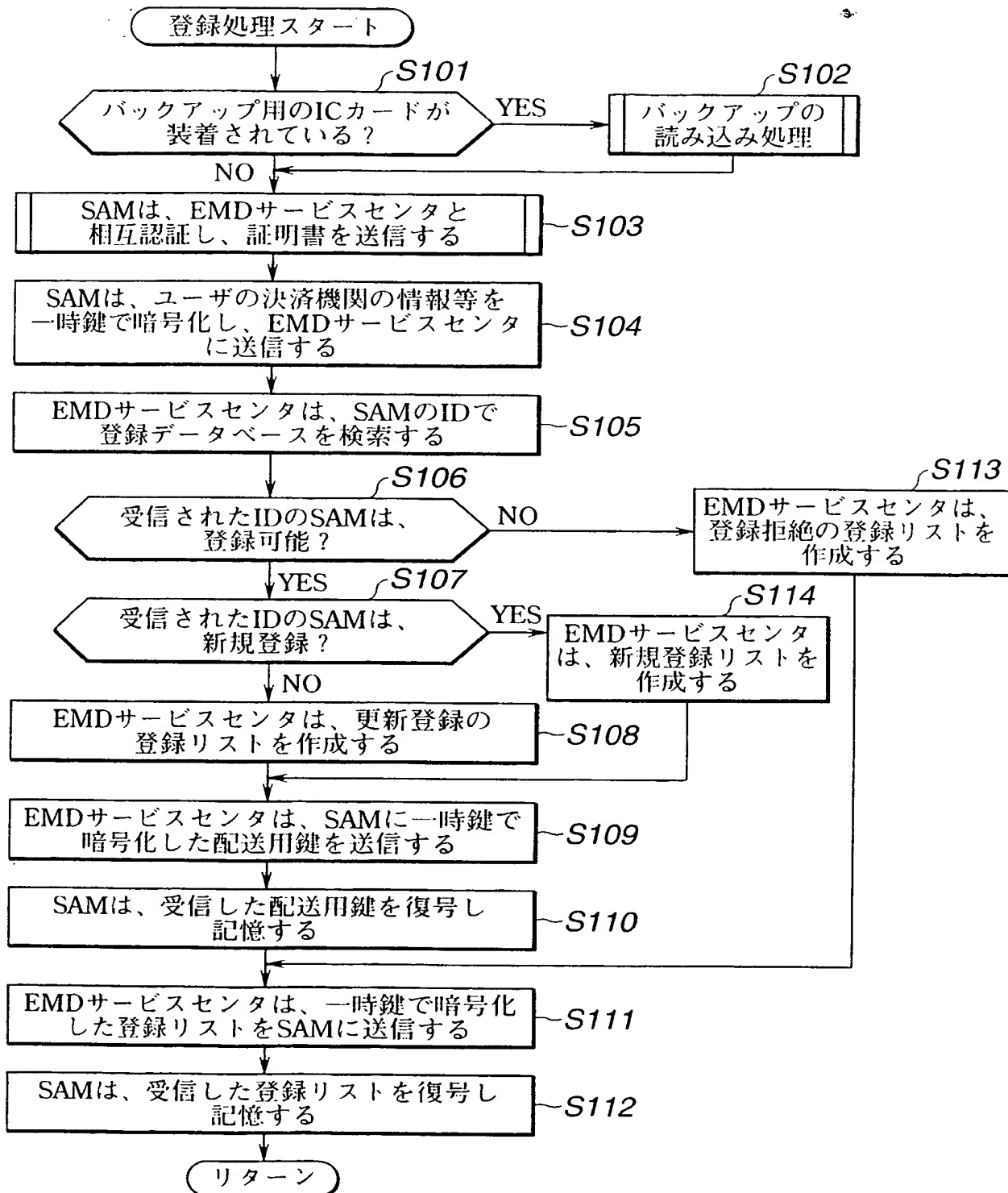


FIG.43

**THIS PAGE BLANK (USPTO)**

43/88

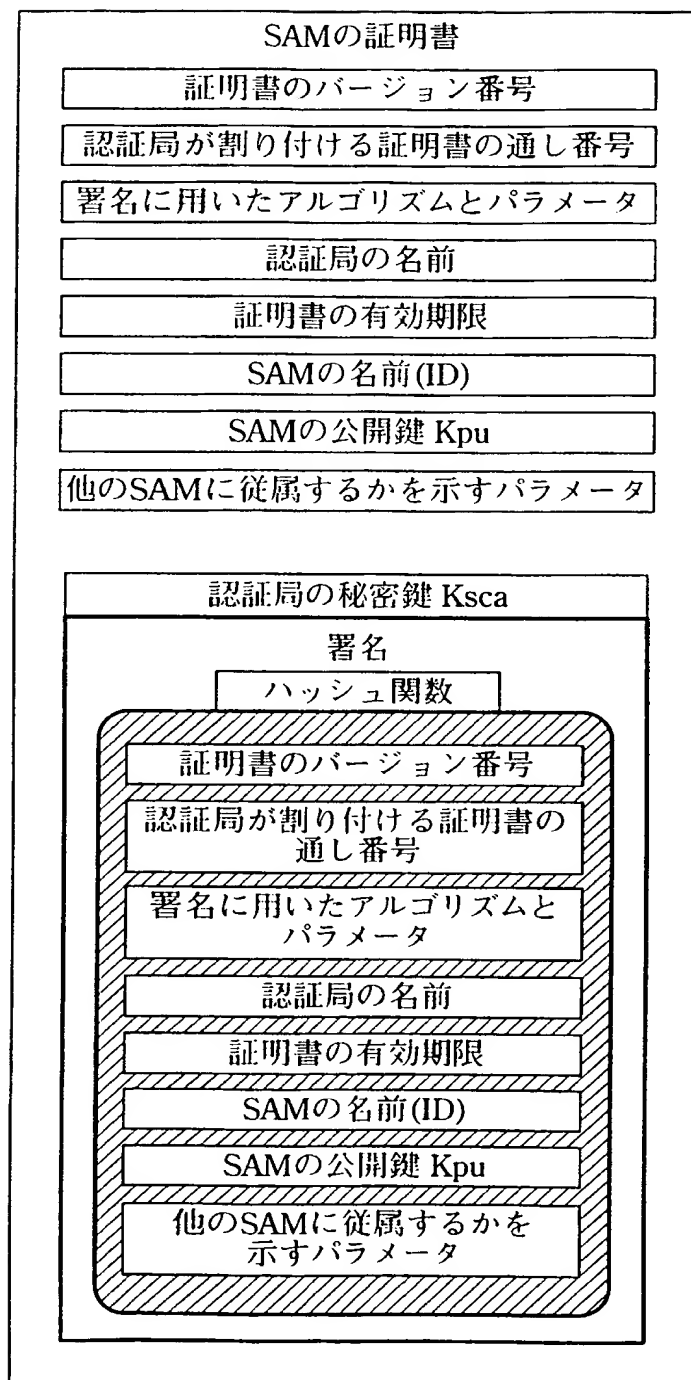


FIG.44

**THIS PAGE BLANK (USPTO)**

SAMのID (64bit)	登録拒絶フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (1bit)	署名
000000000000000001h	1	0000	0	XXXXXXXXXXXX
000000000000000002h	1	1010	1	XXXXXXXXXXXX
000000000000000003h	1	1100	1	XXXXXXXXXXXX
00000000000000000Ah	0	0000	1	XXXXXXXXXXXX

**FIG. 45**

**THIS PAGE BLANK (USPTO)**



45/88

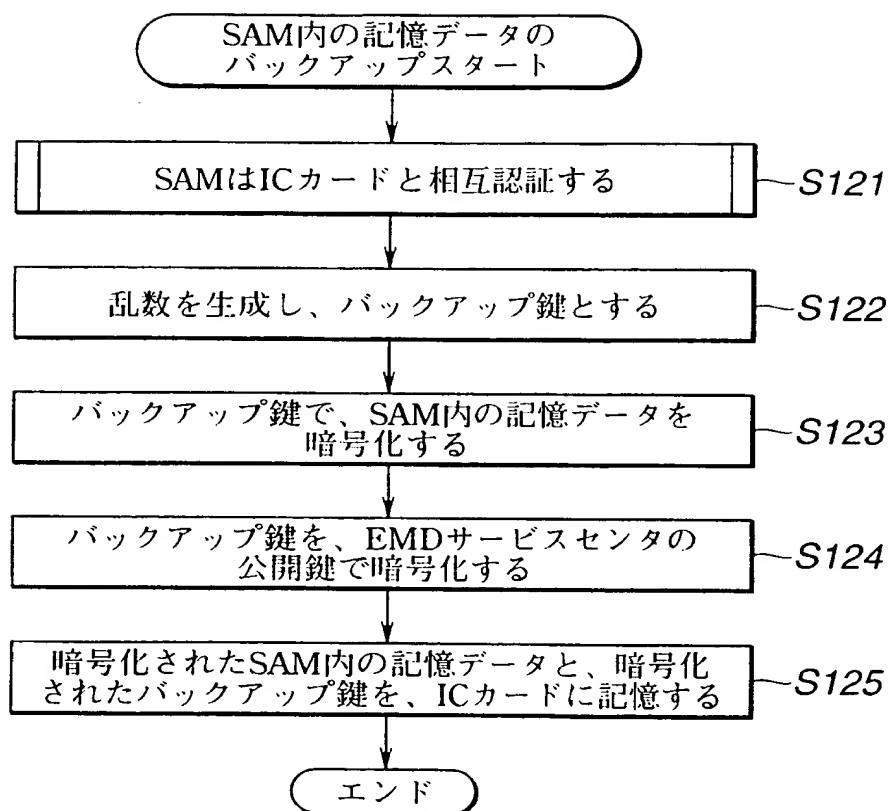


FIG.46

**THIS PAGE BLANK (USPTO)**

46/88

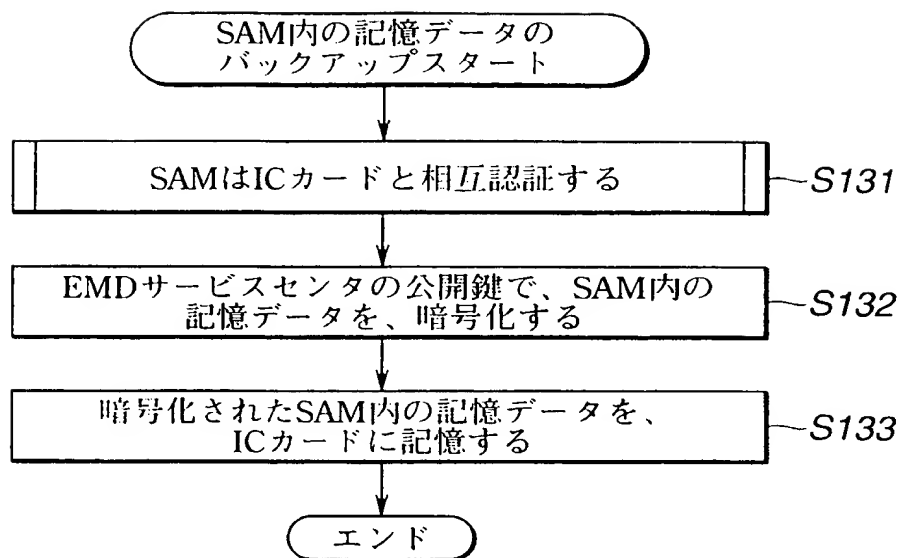


FIG.47

**THIS PAGE BLANK (USPTO)**

---

47/88

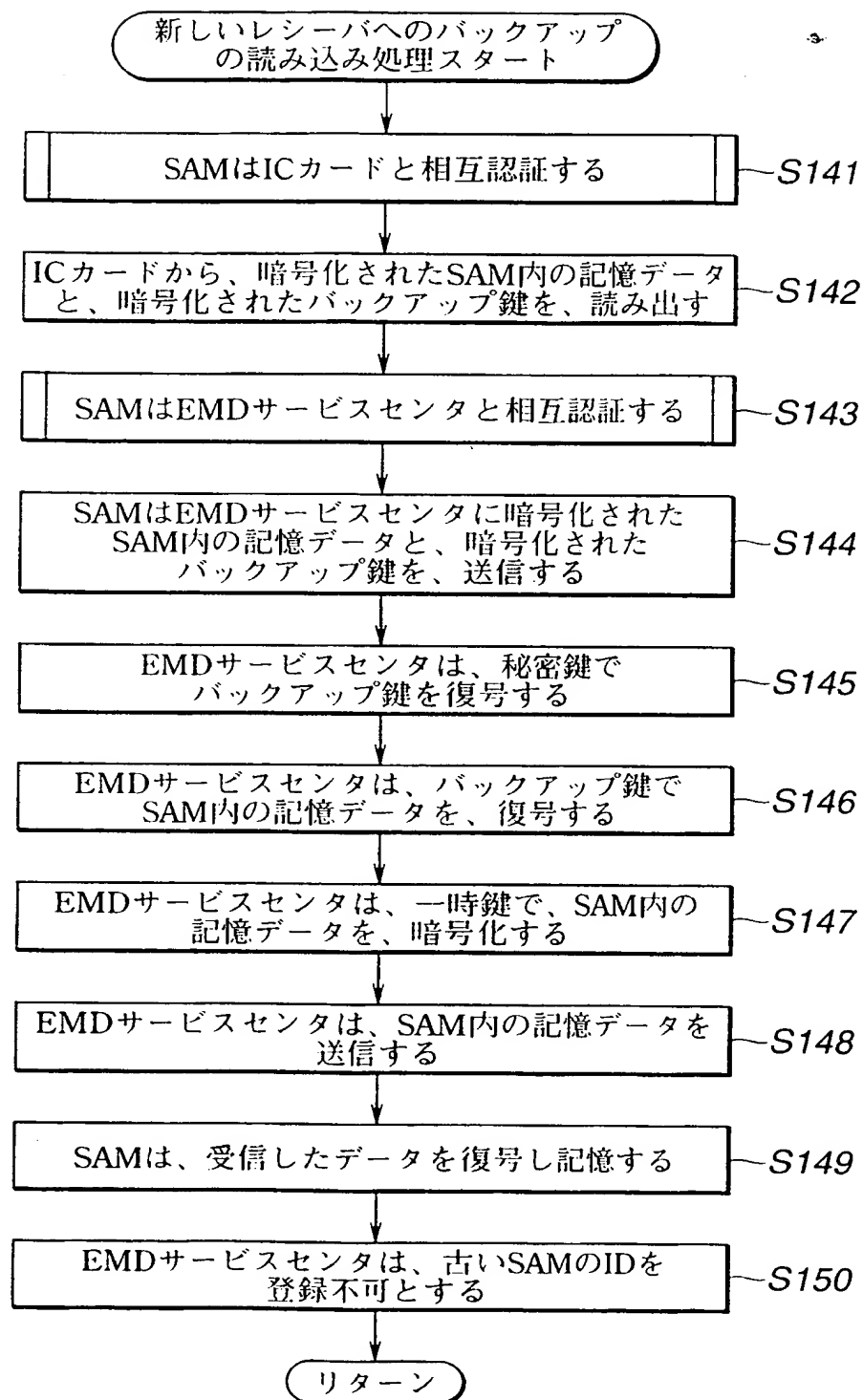


FIG.48

**THIS PAGE BLANK (USPTO)**

---

48/88

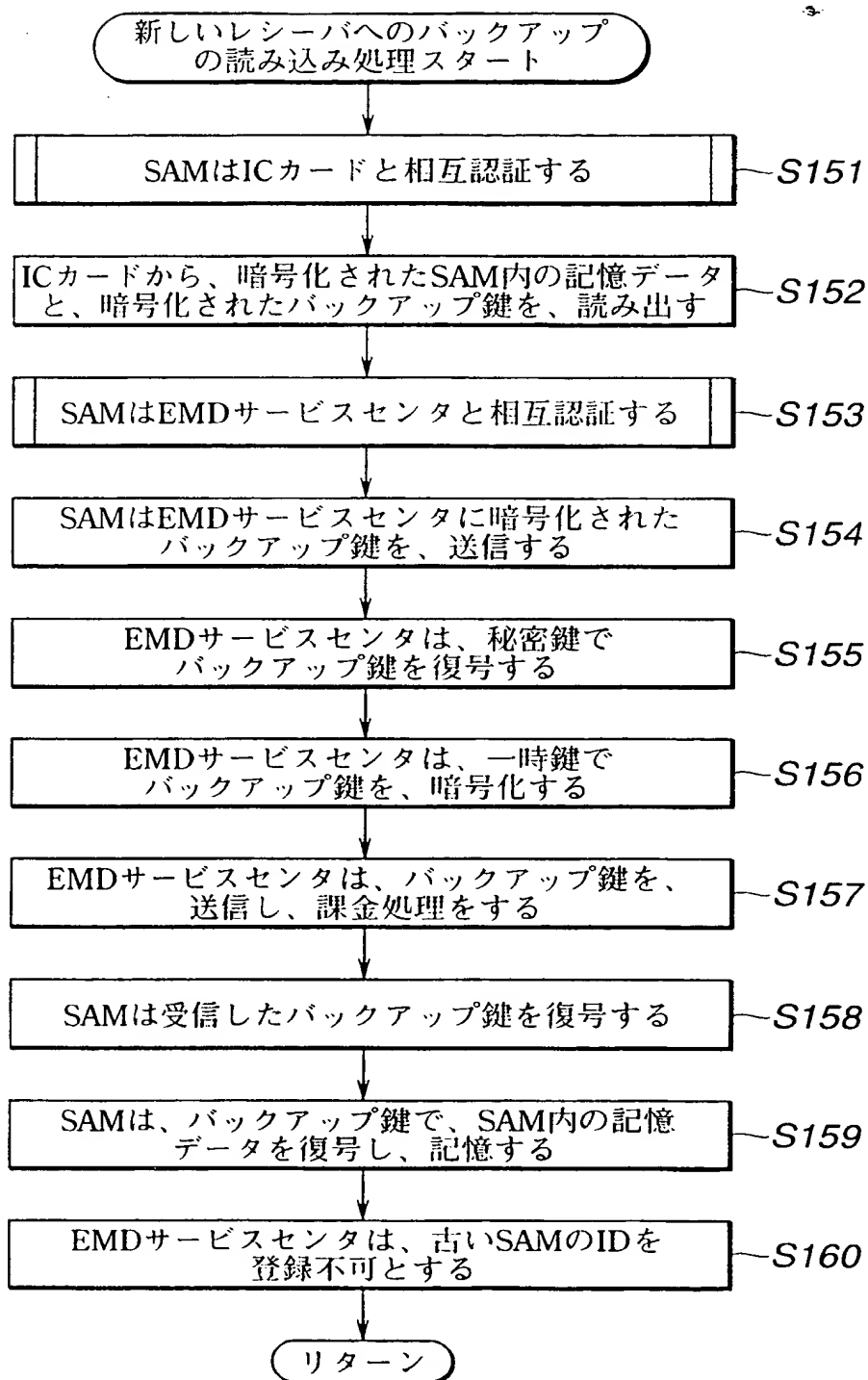


FIG.49

**THIS PAGE BLANK (USPTO)**



49/88

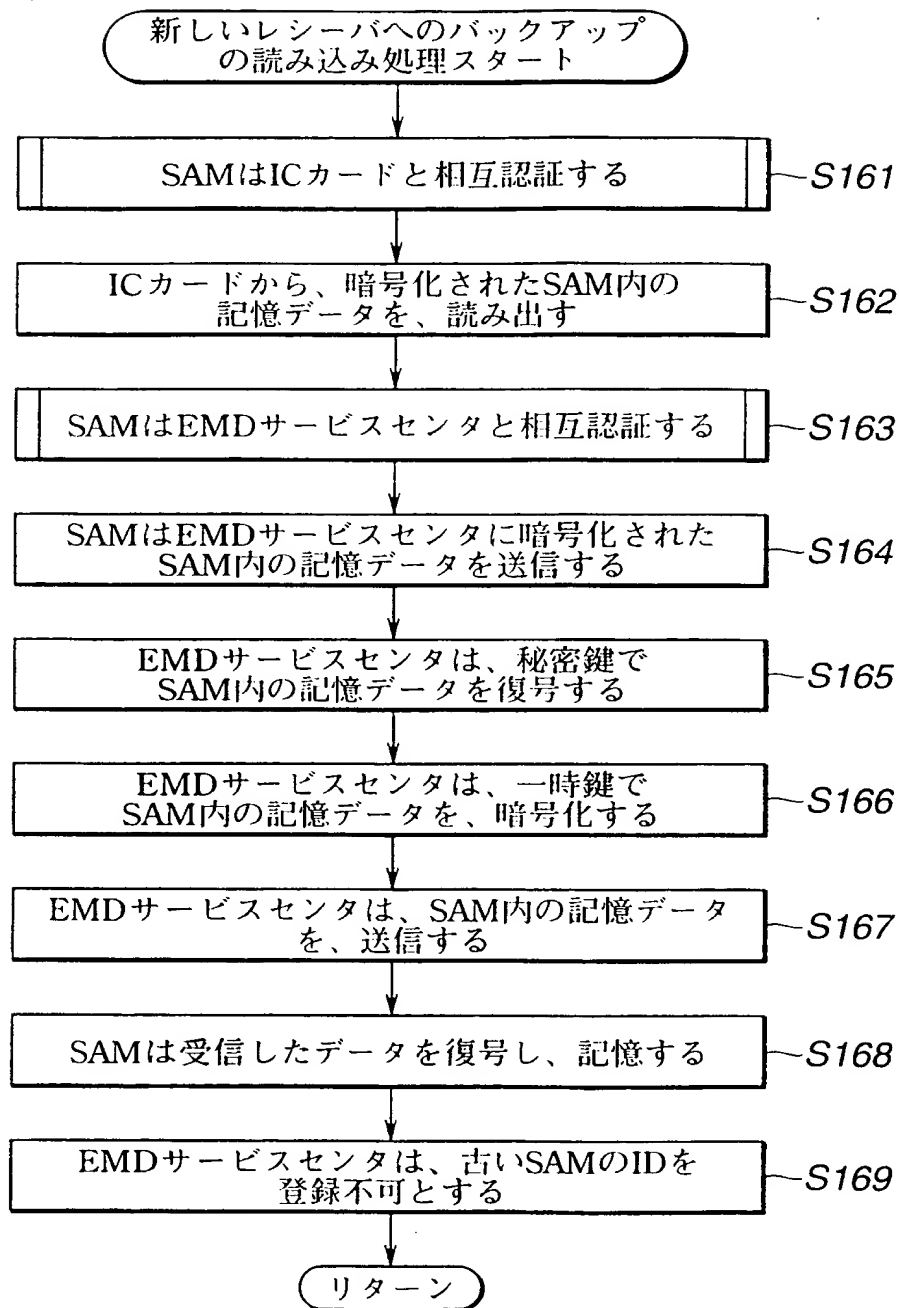


FIG.50

**THIS PAGE BLANK (USPTO)**

---

50/88

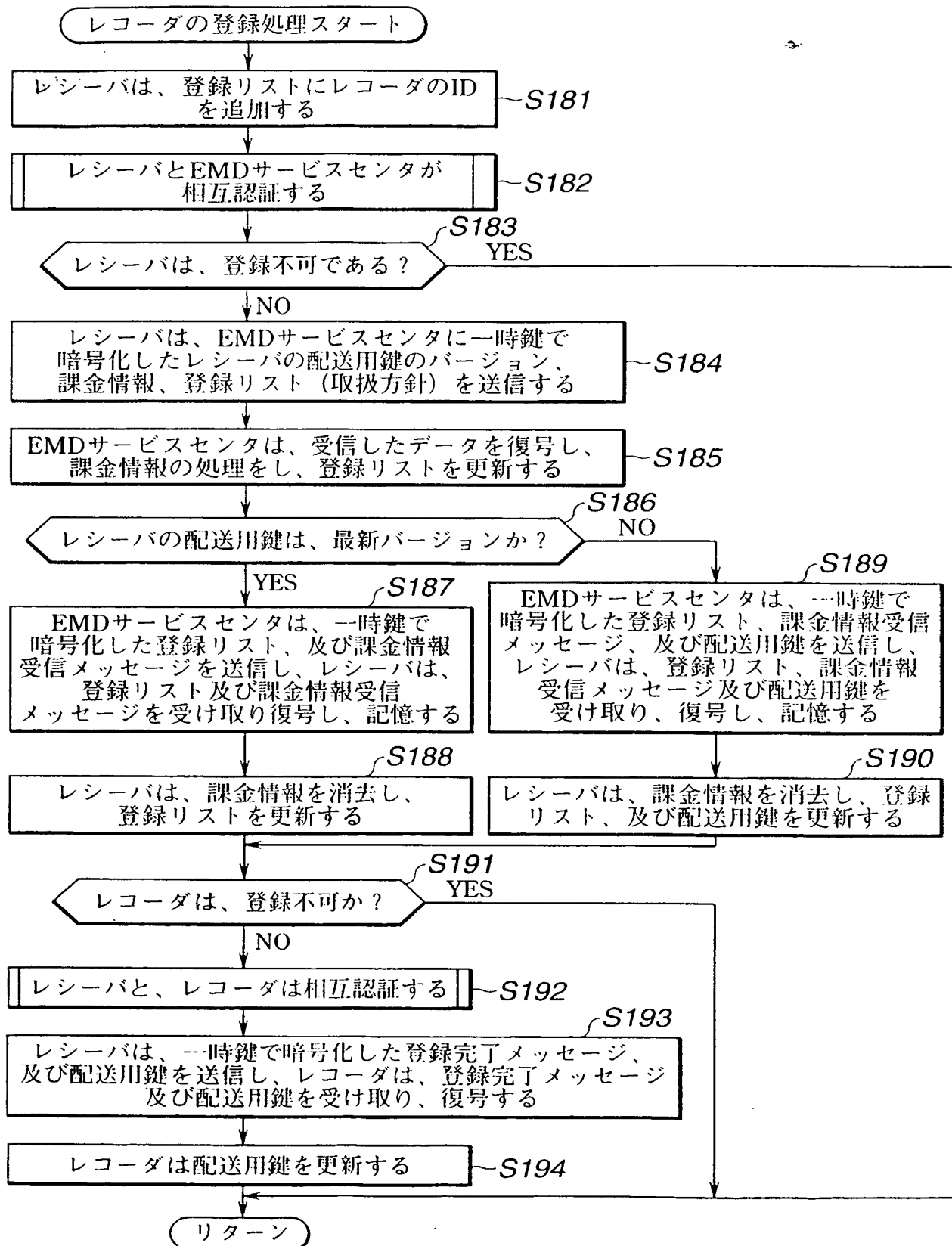


FIG.51

**THIS PAGE BLANK (USPTO)**

51/88

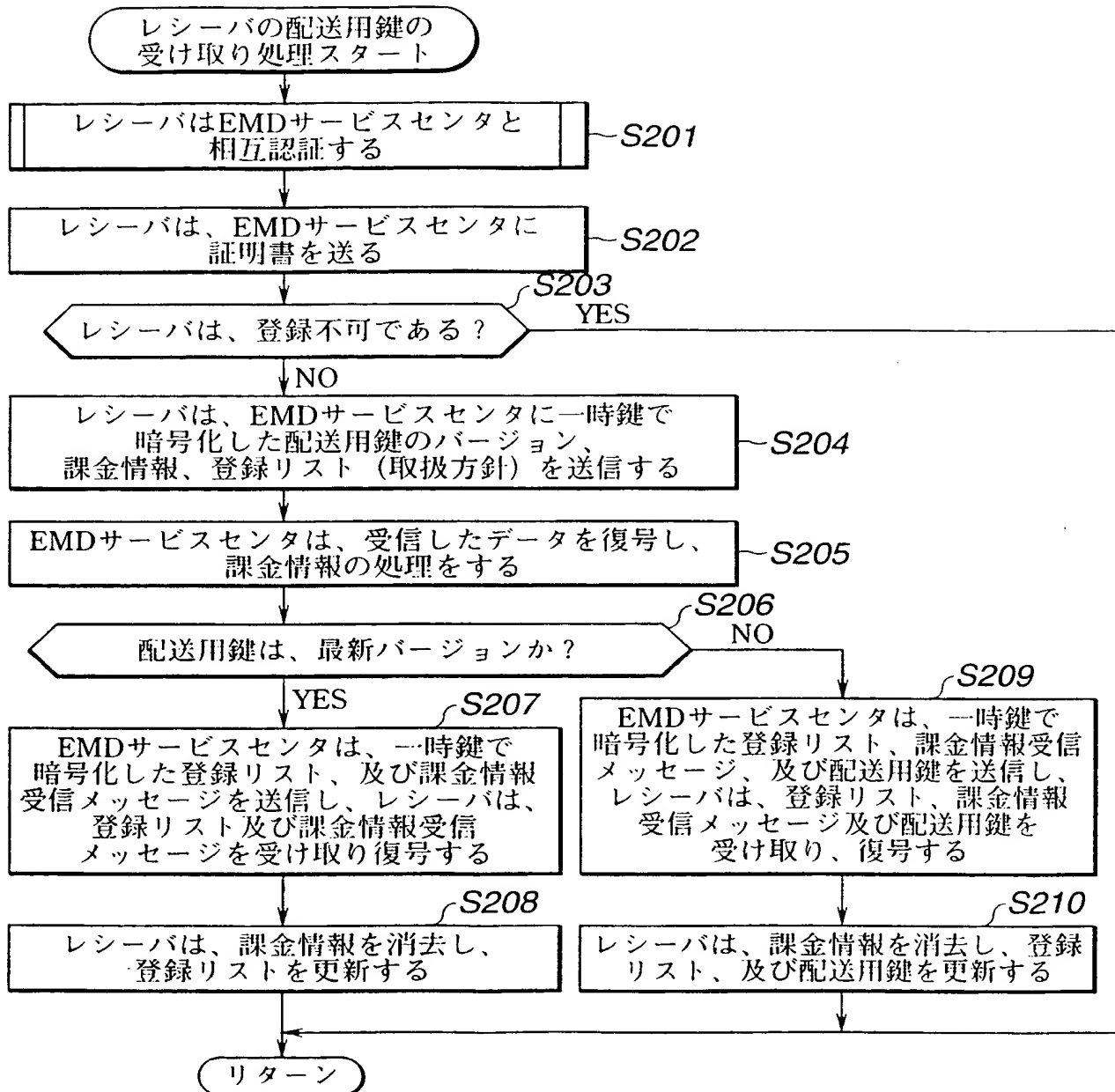


FIG.52

**THIS PAGE BLANK (USPTO)**

52/88

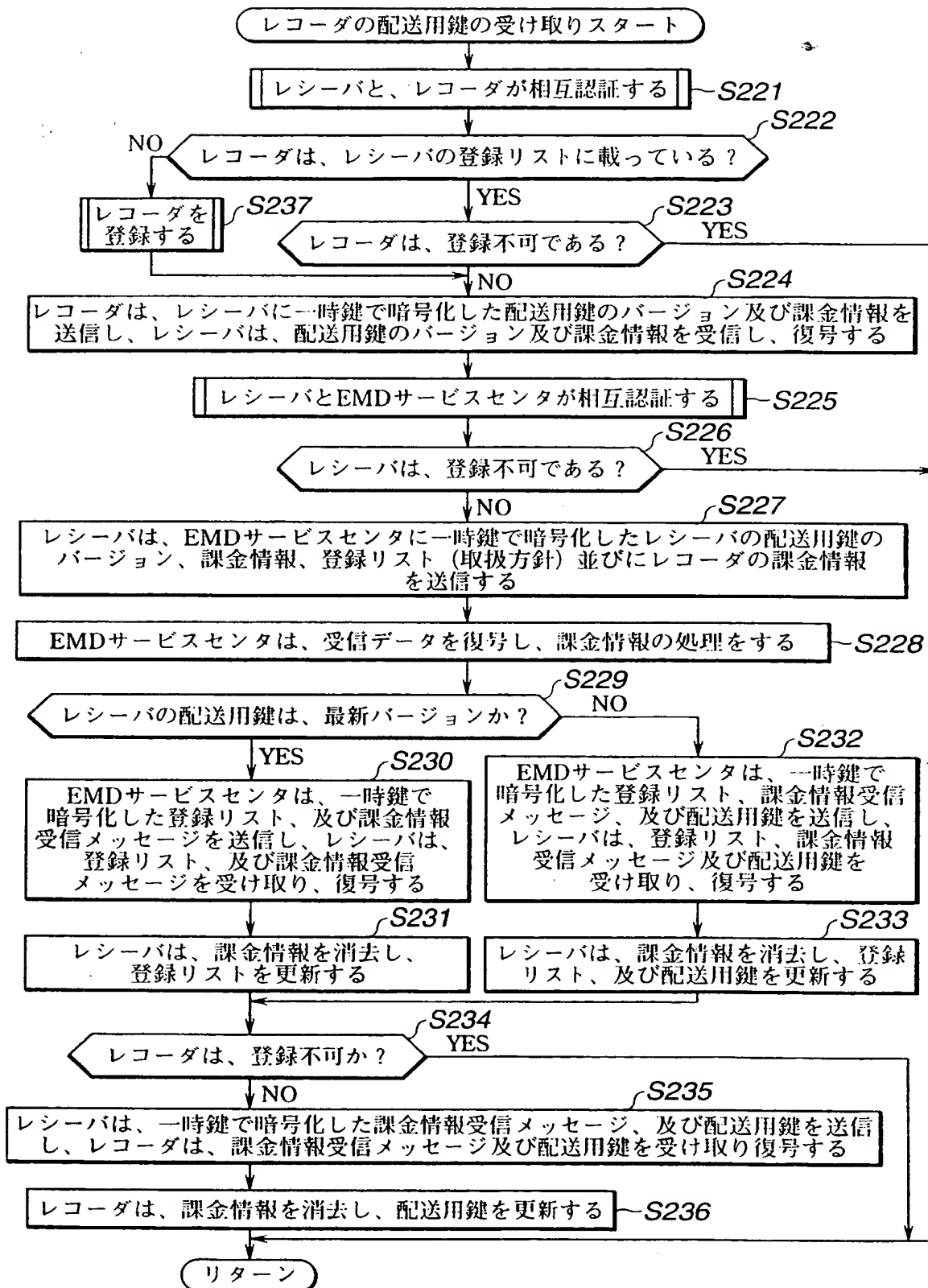


FIG.53

**THIS PAGE BLANK (USPTO)**



53/88

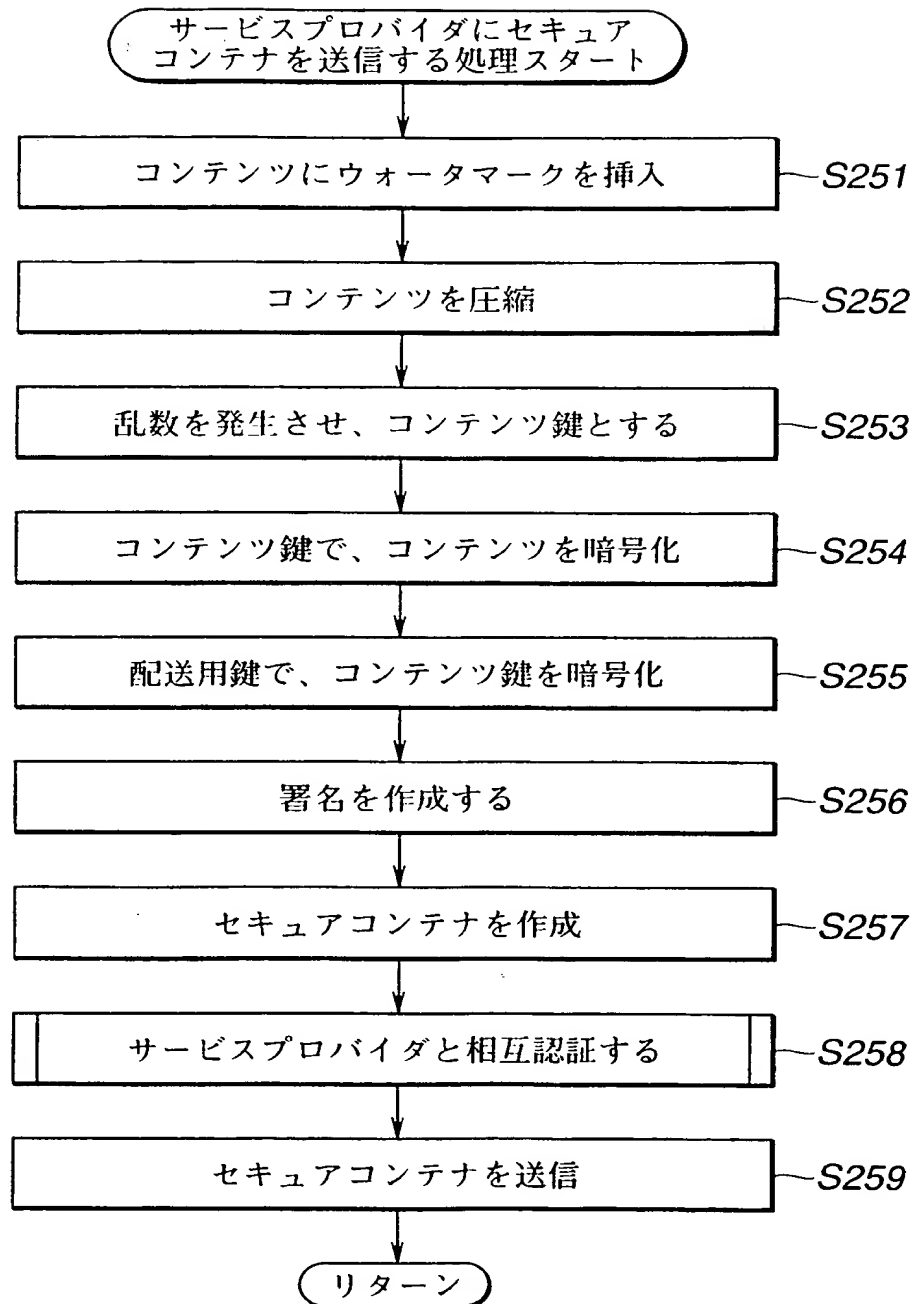


FIG.54

**THIS PAGE BLANK (USPTO)**

54/88

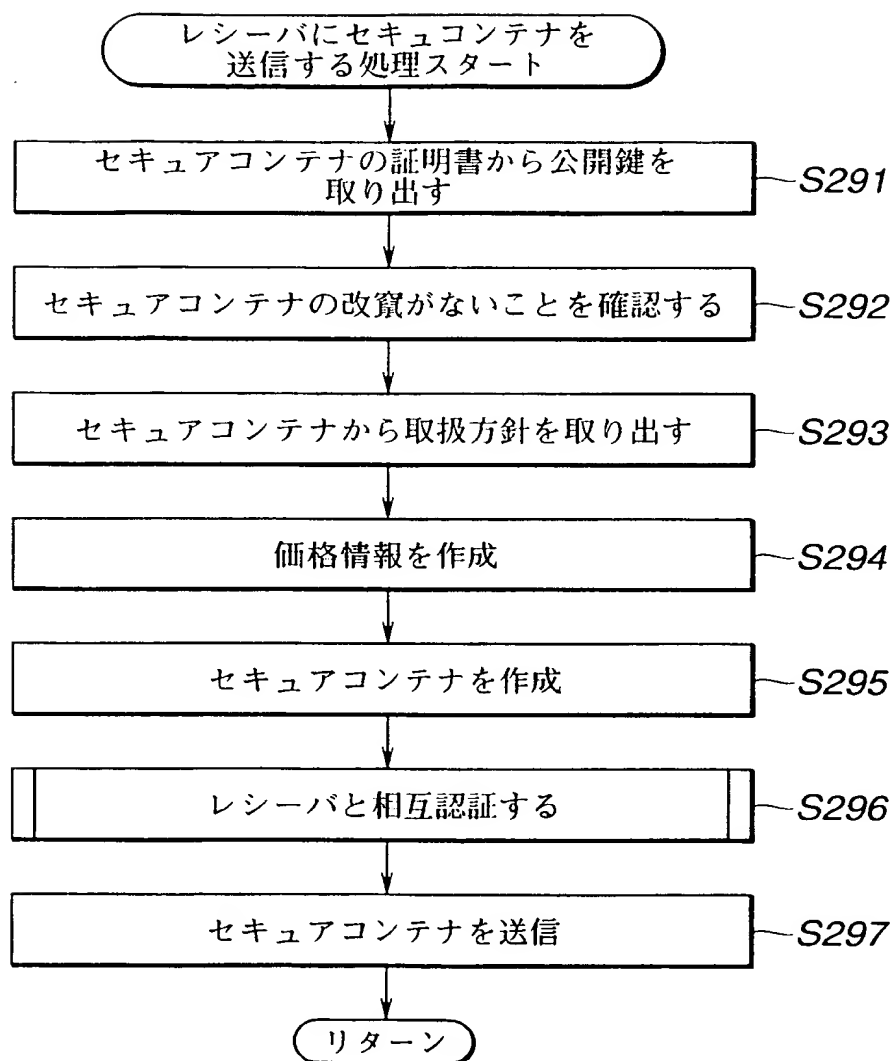


FIG.55

**THIS PAGE BLANK (USPTO)**

55/88

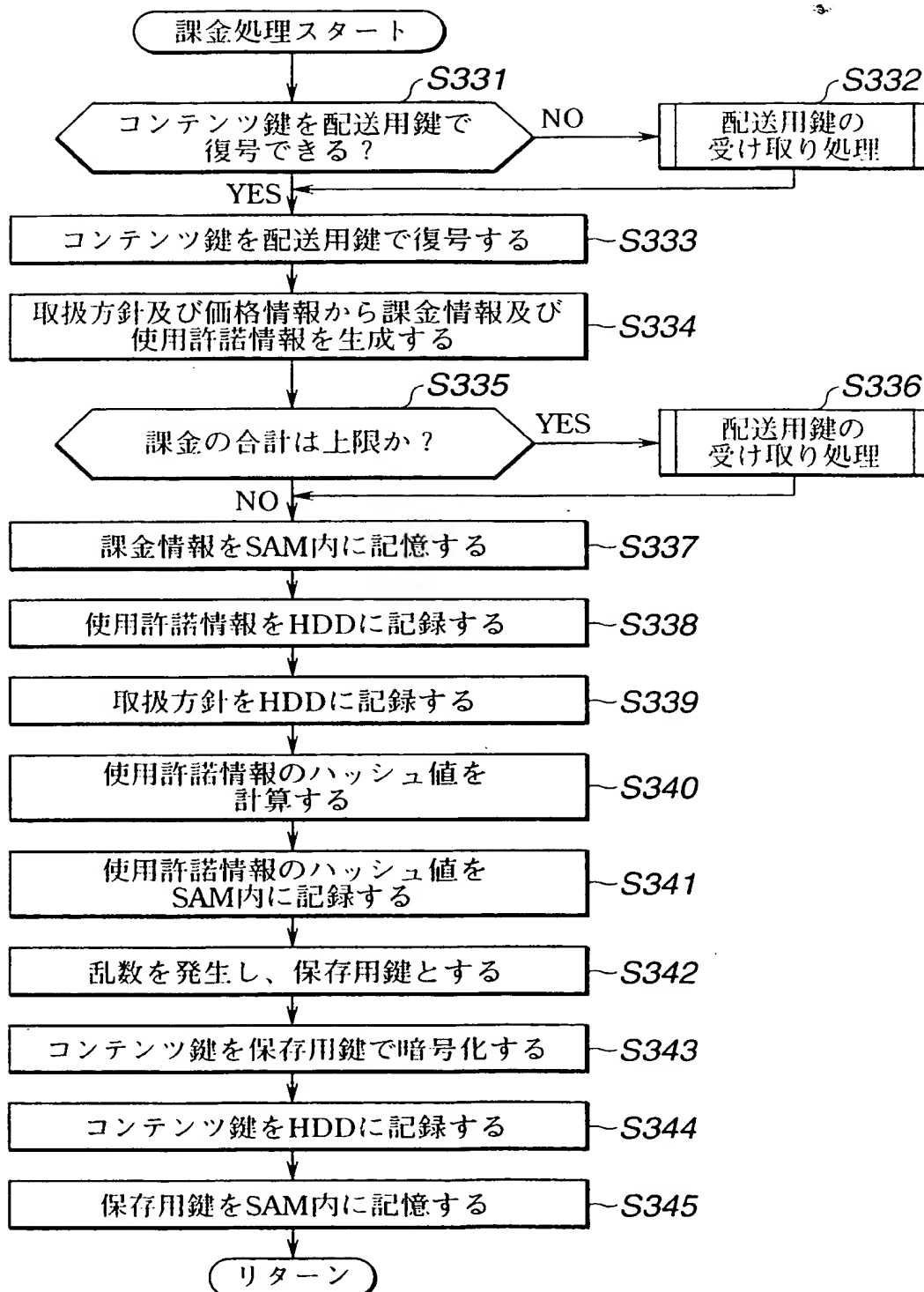


FIG.56

**THIS PAGE BLANK (USPTO)**

---

56/88

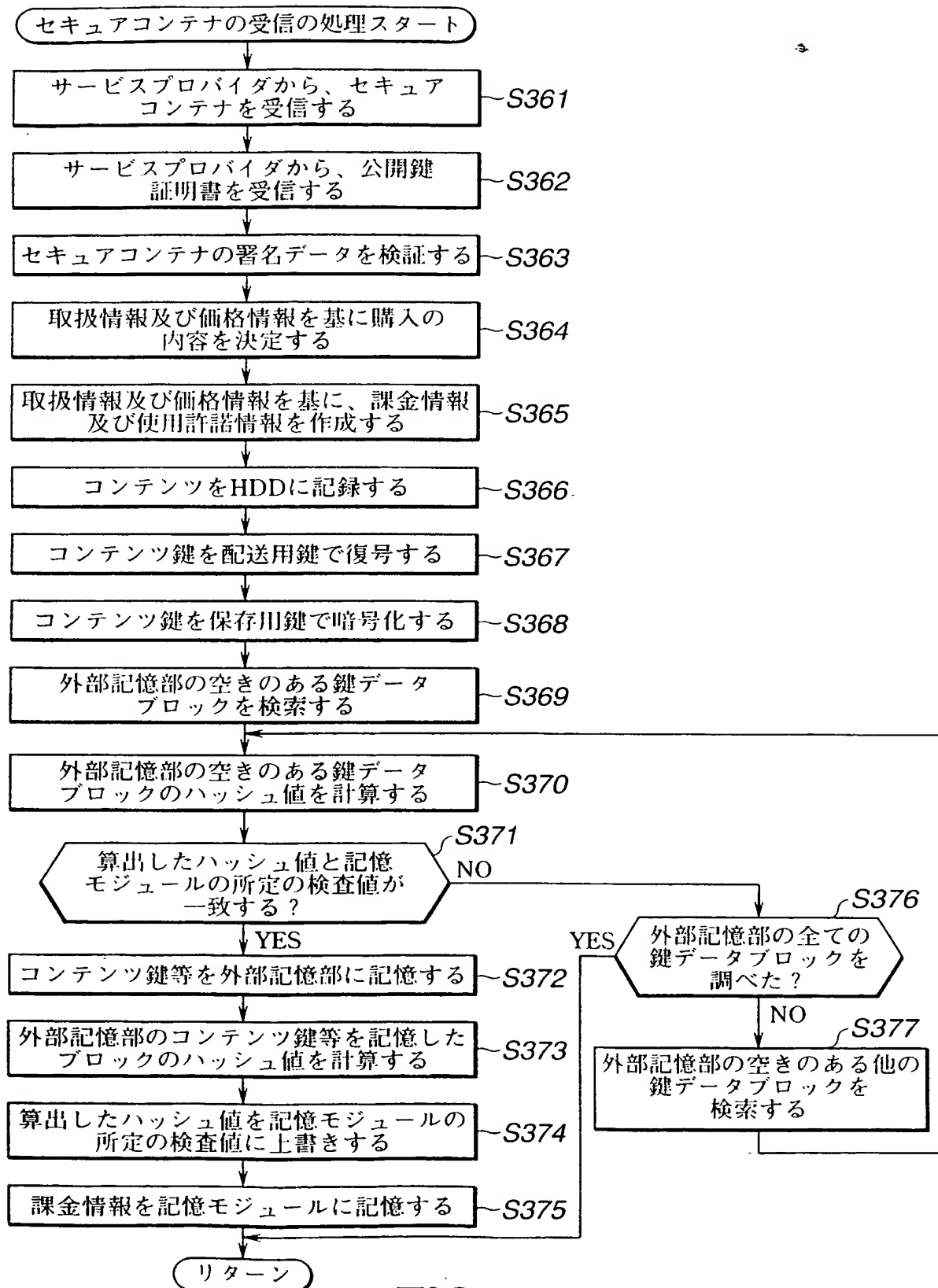


FIG.57

**THIS PAGE BLANK (USPTO)**



57/88

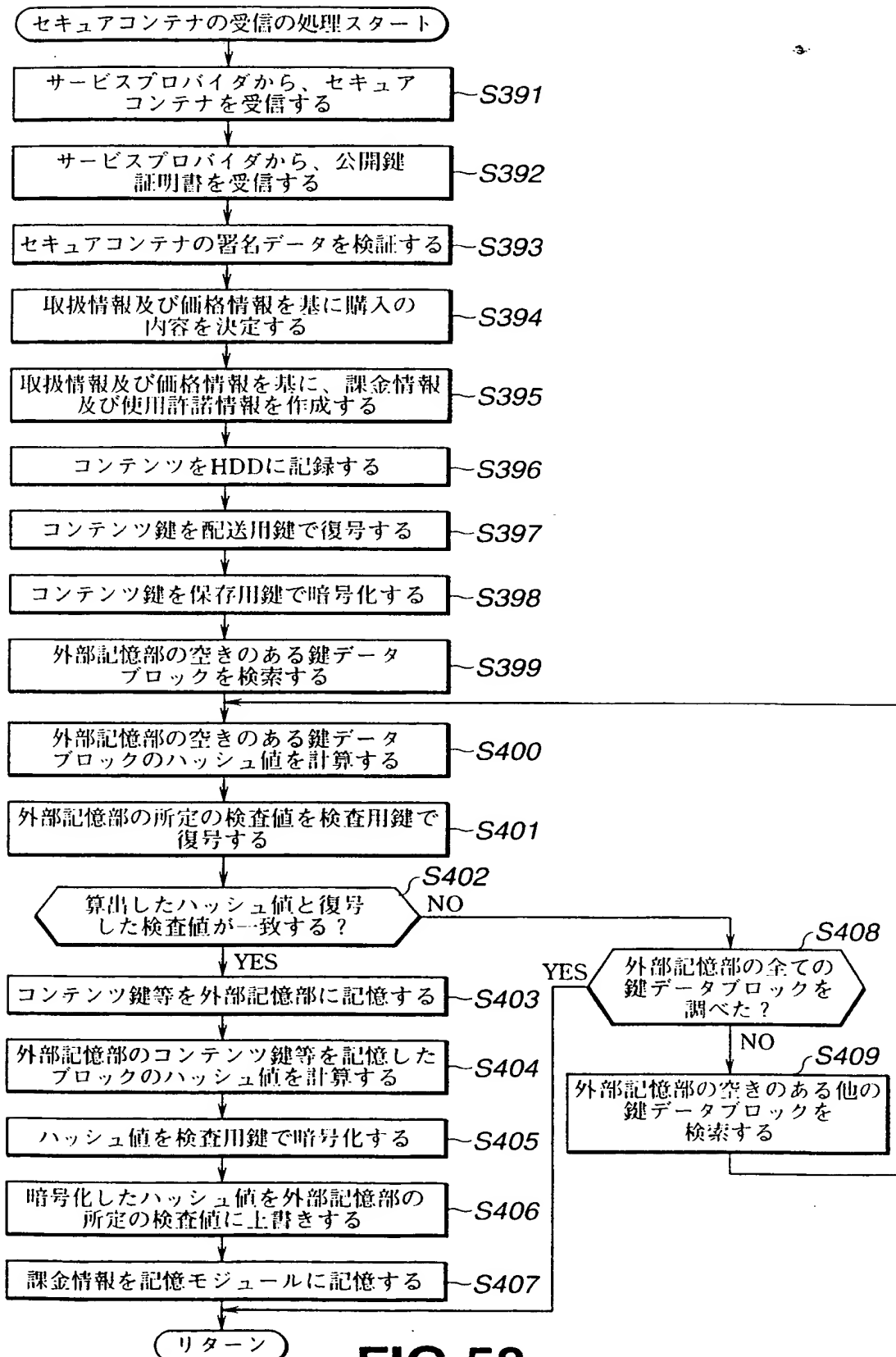


FIG.58

**THIS PAGE BLANK (USPTO)**

---

58/88

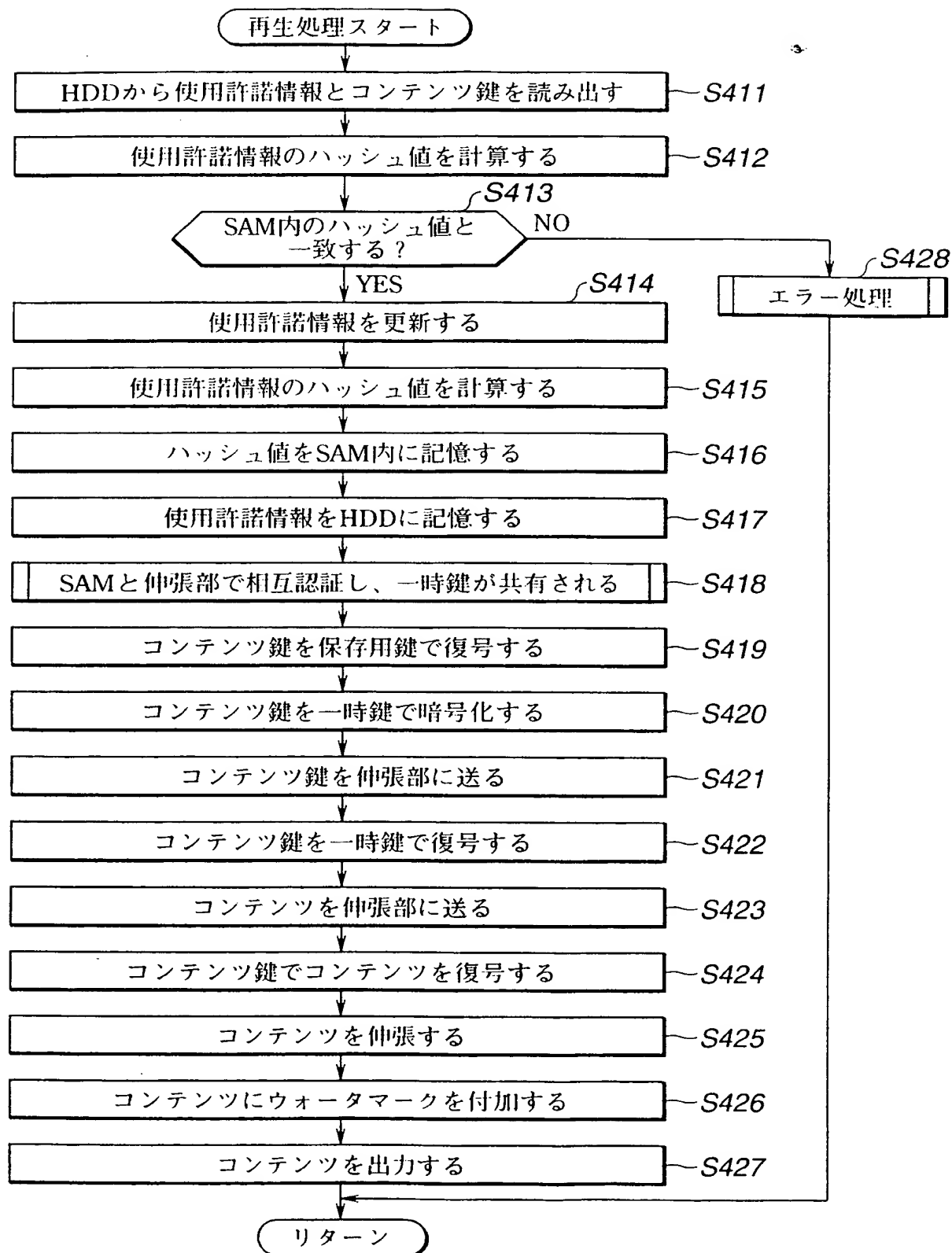


FIG.59

**THIS PAGE BLANK (USPTO)**

---

59/88

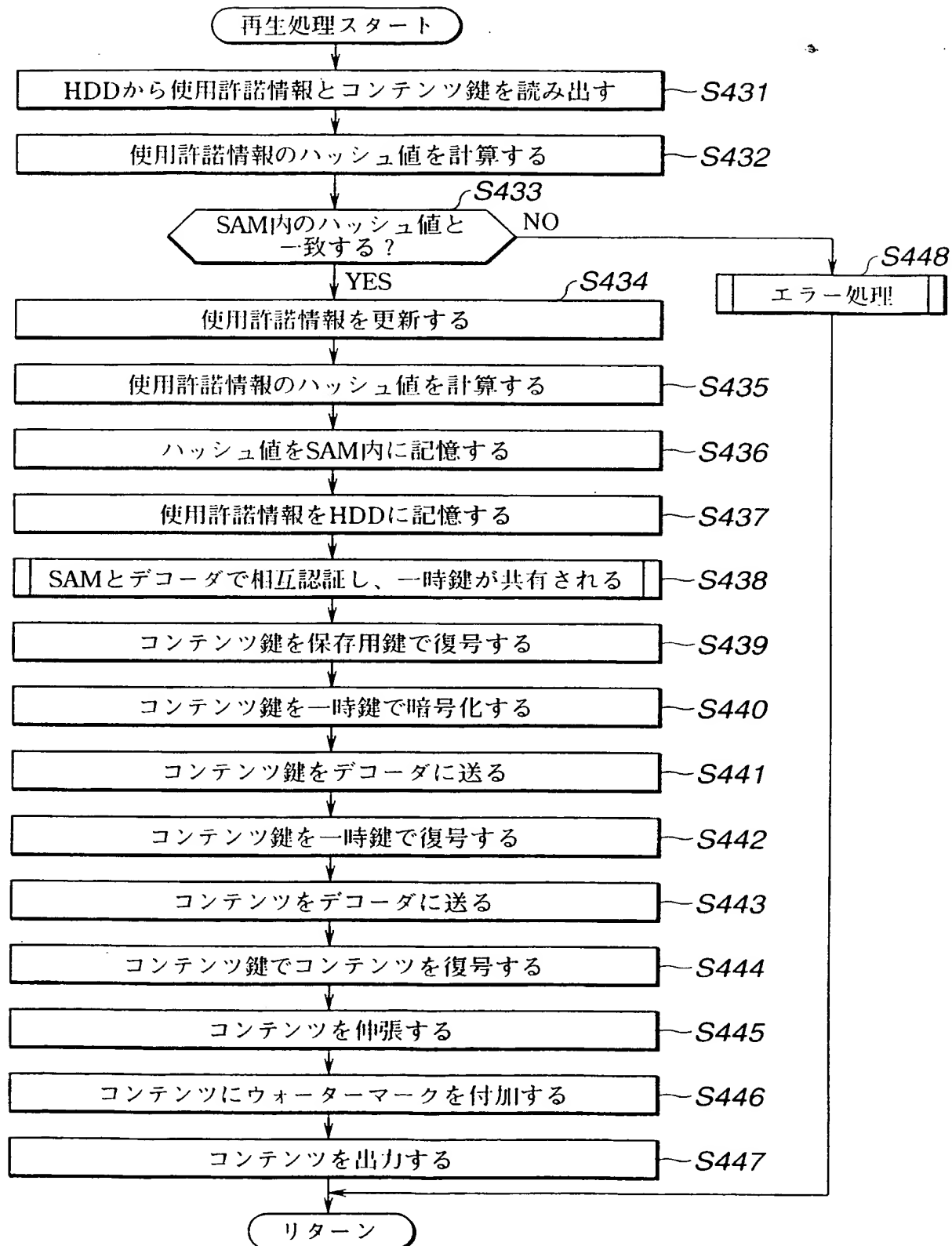


FIG.60

**THIS PAGE BLANK (USPTO)**

60/88

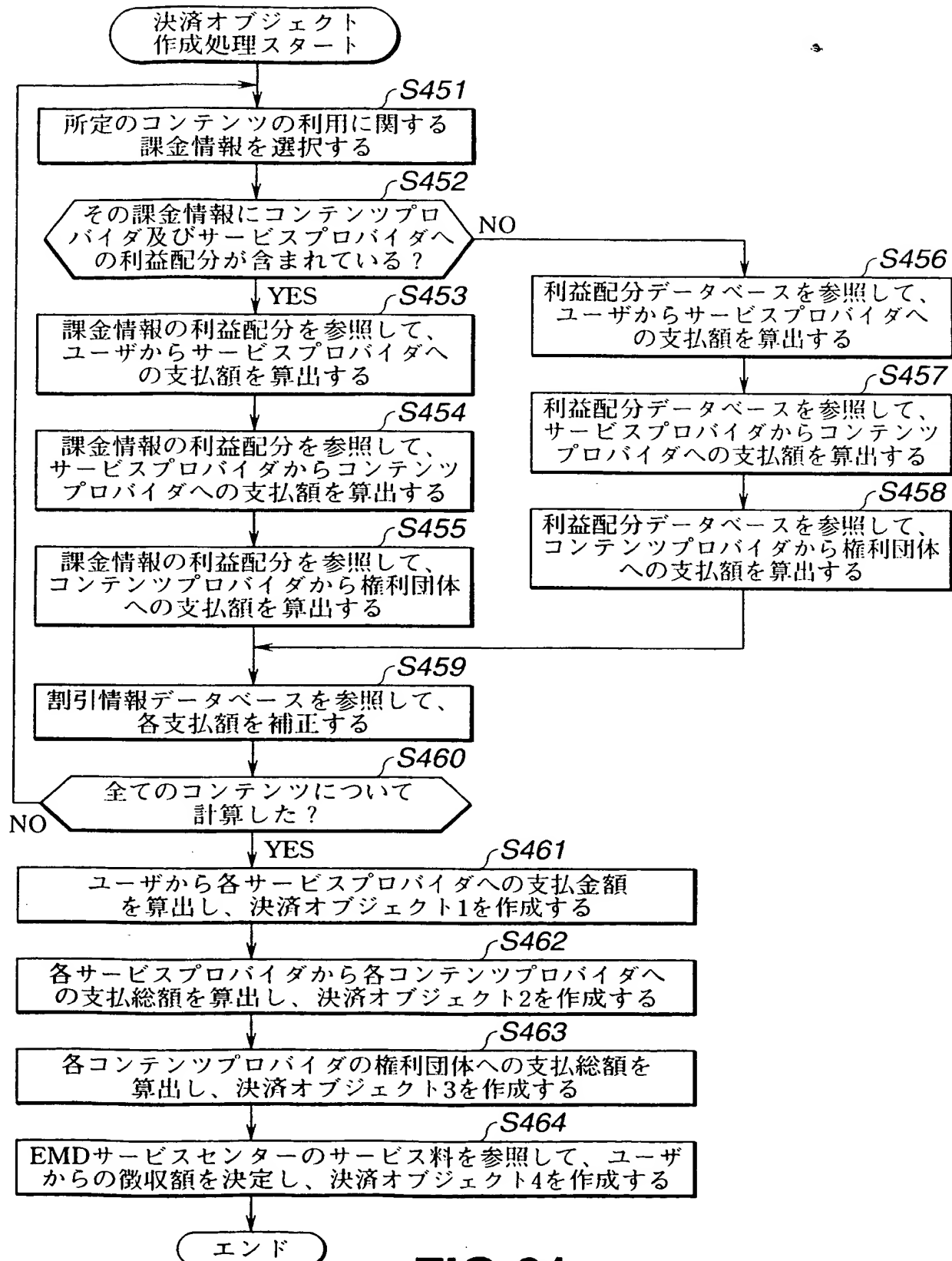


FIG.61

**THIS PAGE BLANK (USPTO)**



61/88

**FIG.62A**クレジット決済  
オブジェクト 1

支払元: ユーザのID  
徴収額: x  
支払先: サービスプロバイダのID  
支払額: x1

**FIG.62B**クレジット決済  
オブジェクト 2

支払元: クレジット決済オブジェクト 1  
徴収額: -  
支払先: コンテンツプロバイダのID  
支払額: x2

**FIG.62C**クレジット決済  
オブジェクト 3

支払元: クレジット決済オブジェクト 1  
徴収額: -  
支払先: 権利団体のID  
支払額: x3

**FIG.62D**クレジット決済  
オブジェクト 4

支払元: クレジット決済オブジェクト 1  
徴収額: -  
支払先: EMDサービスセンタのID  
支払額: x4

**THIS PAGE BLANK (USPTO)**

62/88

**FIG.63A**

銀行決済  
オブジェクト 1

支払元: サービスプロバイダのID  
徴収額: y1  
支払先: EMDサービスセンタのID  
支払額: y1

**FIG.63B**

銀行決済  
オブジェクト 2

支払元: コンテンツプロバイダのID  
徴収額: y2  
支払先: EMDサービスセンタのID  
支払額: y2

**FIG.63C**

銀行決済  
オブジェクト 3

支払元: 権利団体のID  
徴収額: y3  
支払先: EMDサービスセンタのID  
支払額: y3

**THIS PAGE BLANK (USPTO)**

63/88

**FIG.64A**クレジット決済  
オブジェクト 1

支払元: ユーザのID  
徴収額: x  
支払先: サービスプロバイダのID  
支払額: x1

**FIG.64B**銀行決済  
オブジェクト 2

支払元: サービスプロバイダのID  
徴収額:  $x2 + x3$   
支払先: コンテンツプロバイダのID  
支払額:  $x2 + x3$

**FIG.64C**銀行決済  
オブジェクト 3

支払元: コンテンツプロバイダのID  
徴収額:  $x3$   
支払先: 権利団体のID  
支払額:  $x3$

**FIG.64D**クレジット決済  
オブジェクト 4

支払元: クレジット決済オブジェクト 1  
徴収額: -  
支払先: EMDサービスセンタのID  
支払額:  $x4$

**THIS PAGE BLANK (USPTO)**

64/88

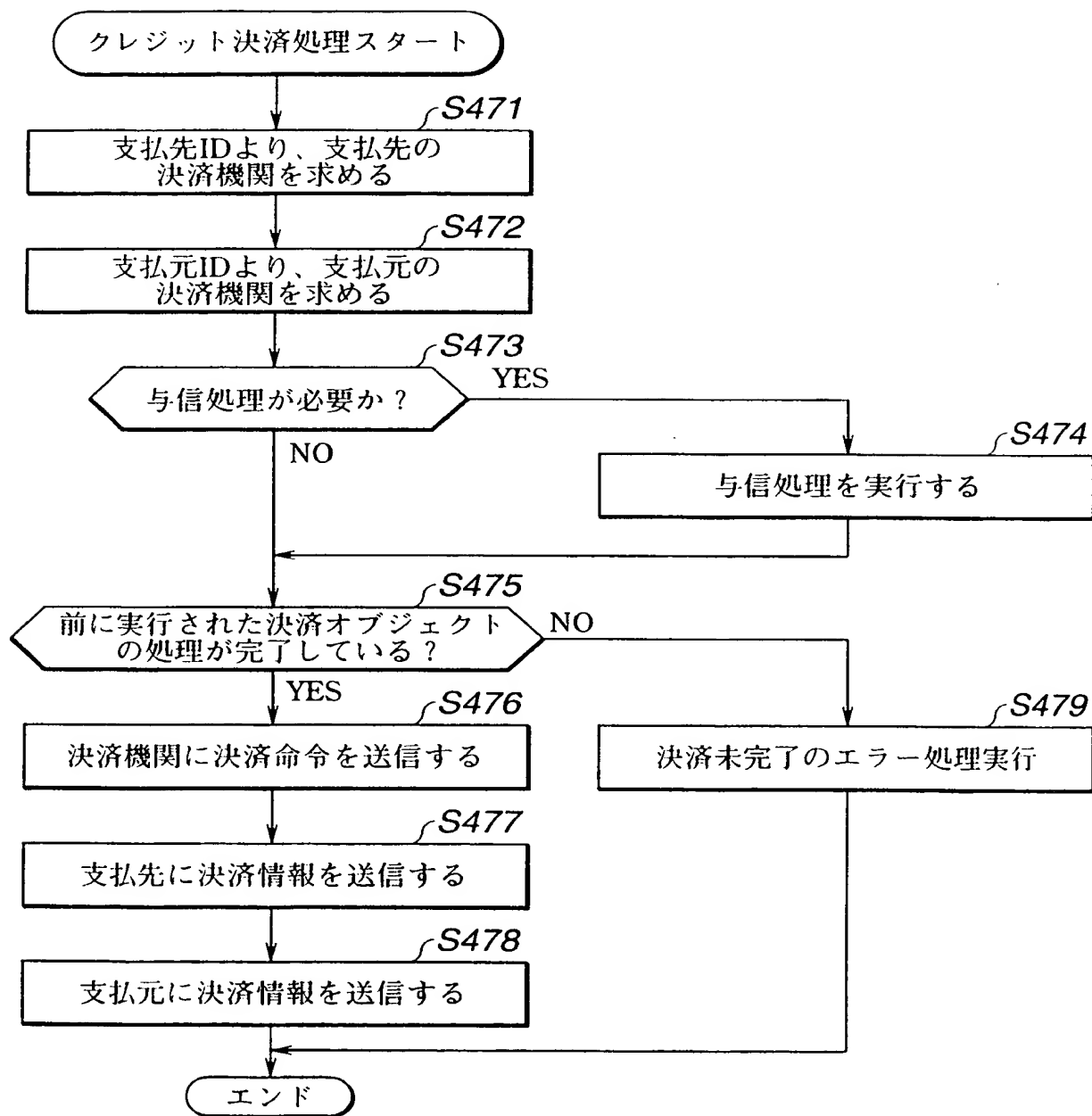


FIG.65

**THIS PAGE BLANK (USPTO,**



65/88

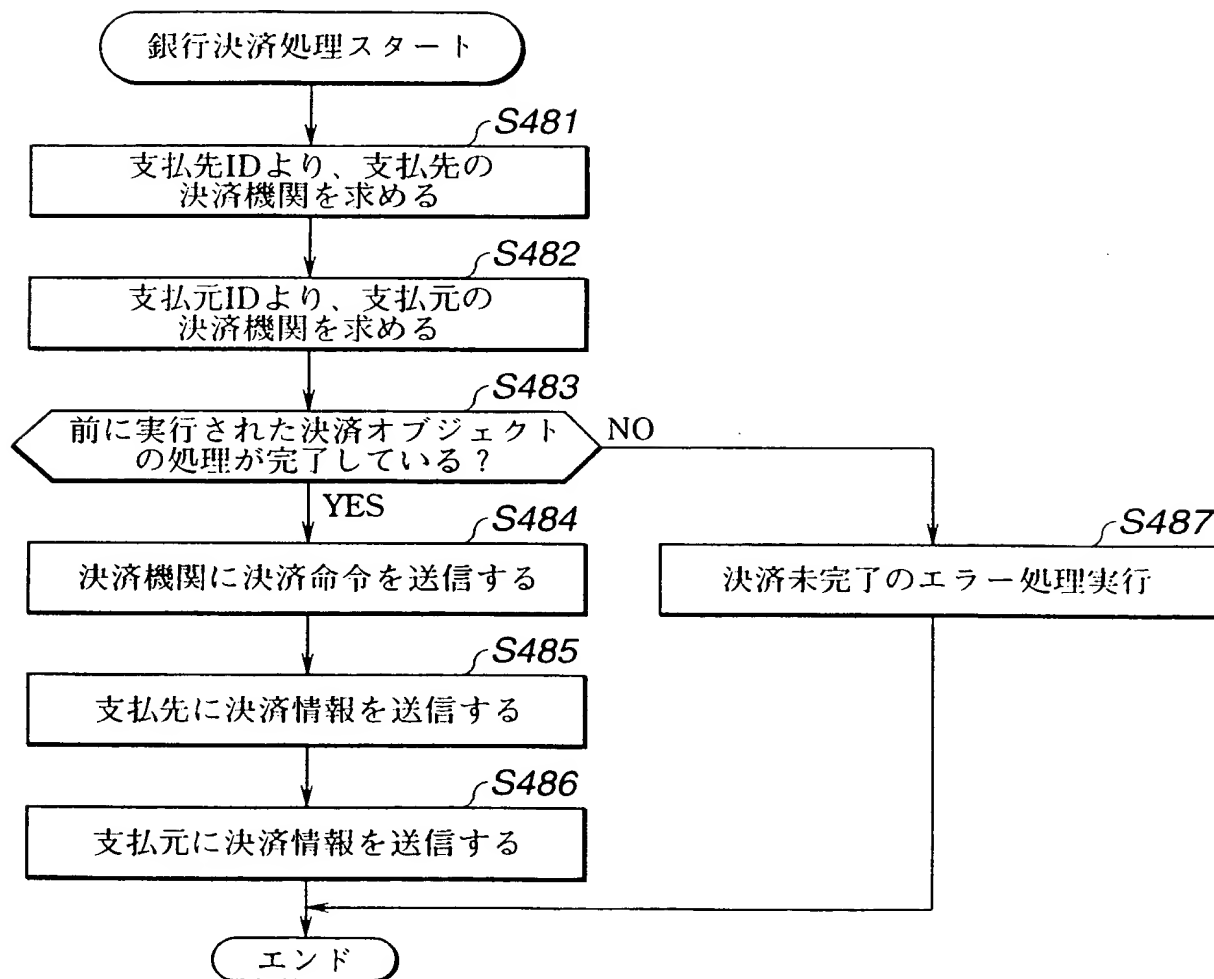


FIG.66

**THIS PAGE BLANK (USPTO)**

66/88

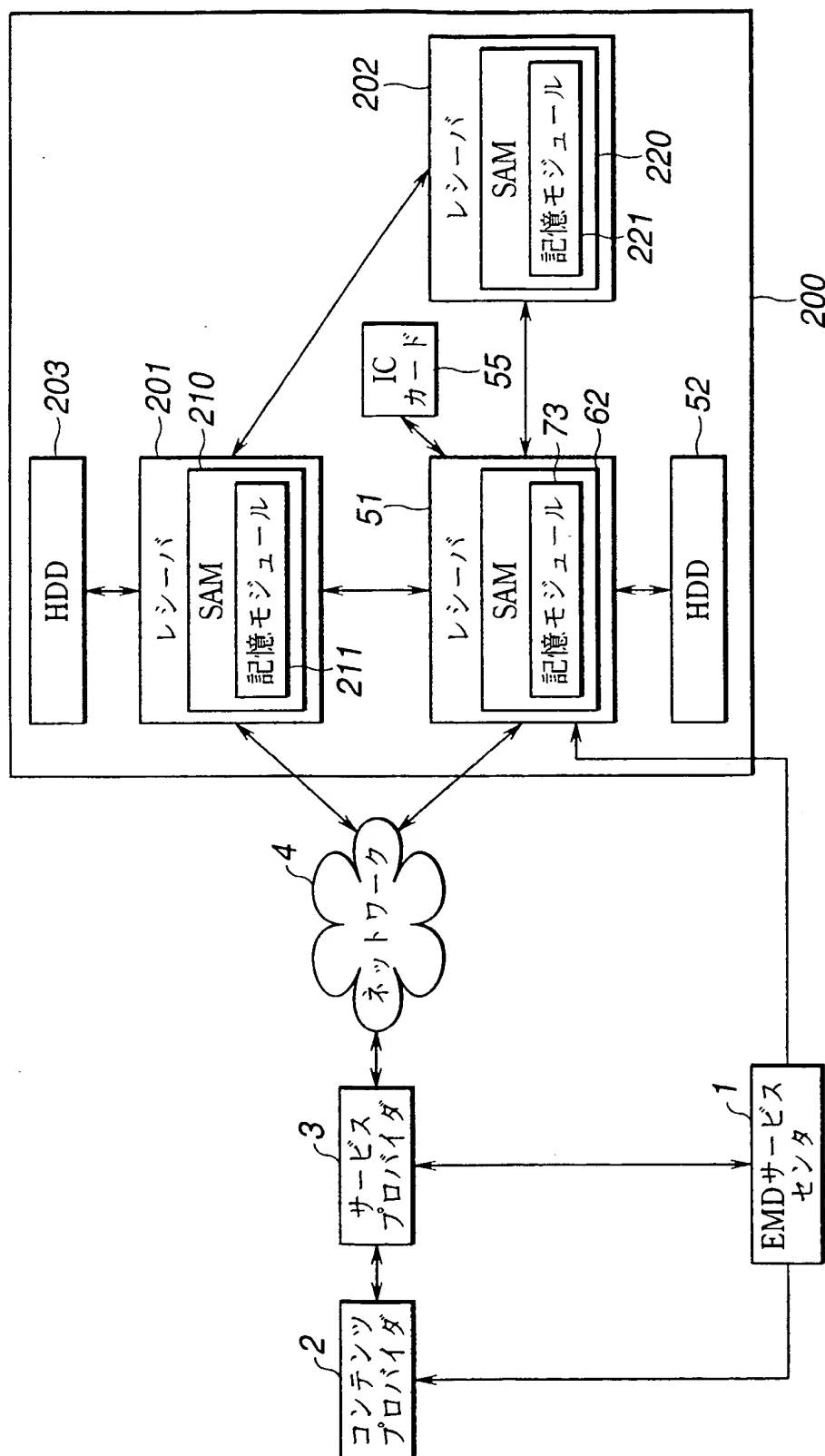


FIG.67

**THIS PAGE BLANK (USPTO)**

---

リスト部									
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態情報	登録条件署名	登録リスト署名	
レシーババ51の登録条件 SAM62のID	ユーザのID	可	可	SAM62のID	なし	制限なし	XXX	XXXX	
レシーババ201の登録条件 SAM210のID	ユーザのID	可	不可	SAM62のID	なし	制限なし	XXX		
レシーババ202の登録条件 SAM220のID	ユーザのID	不可	不可	なし	SAM62のID SAM210のID	制限なし	XXX		

対象SAM ID

SAM62のID

有効期限

XXXX

バージョン番号

XXXX

接続されている機器数

3

対象SAM情報部

FIG.68

**THIS PAGE BLANK (USPTO)**

リスト部									
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態情報	登録条件署名	登録リスト署名	
レシーバ51の登録条件 レシーバ201の登録条件 レシーバ202の登録条件	ユーザのID ユーザのID ユーザのID	可 可 不可	可 不可 不可	SAM62のID SAM62のID なし	なし なし SAM62のID SAM210のID	制限なし 制限なし 制限なし	×××× ×××× ××××	×××××   	

対象SAM ID

SAM210のID

有効期限

×××××

バージョン番号

×××××

接続されている機器数

3

対象SAM情報部

FIG.69

**THIS PAGE BLANK (USPTO)**



レシーバ202の登録条件

SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態情報	登録条件署名	登録リスト署名
SAM220のID	ユーザのID	不可	不可	なし	SAM62のID SAM210のID	制限なし	XXX	XXXX

リスト部

対象SAM ID

SAM220のID

有効期限

XXXX

バージョン番号

XXXX

接続されている機器数

3

対象SAM情報部

FIG.70

**THIS PAGE BLANK (USPTO)**

70/88

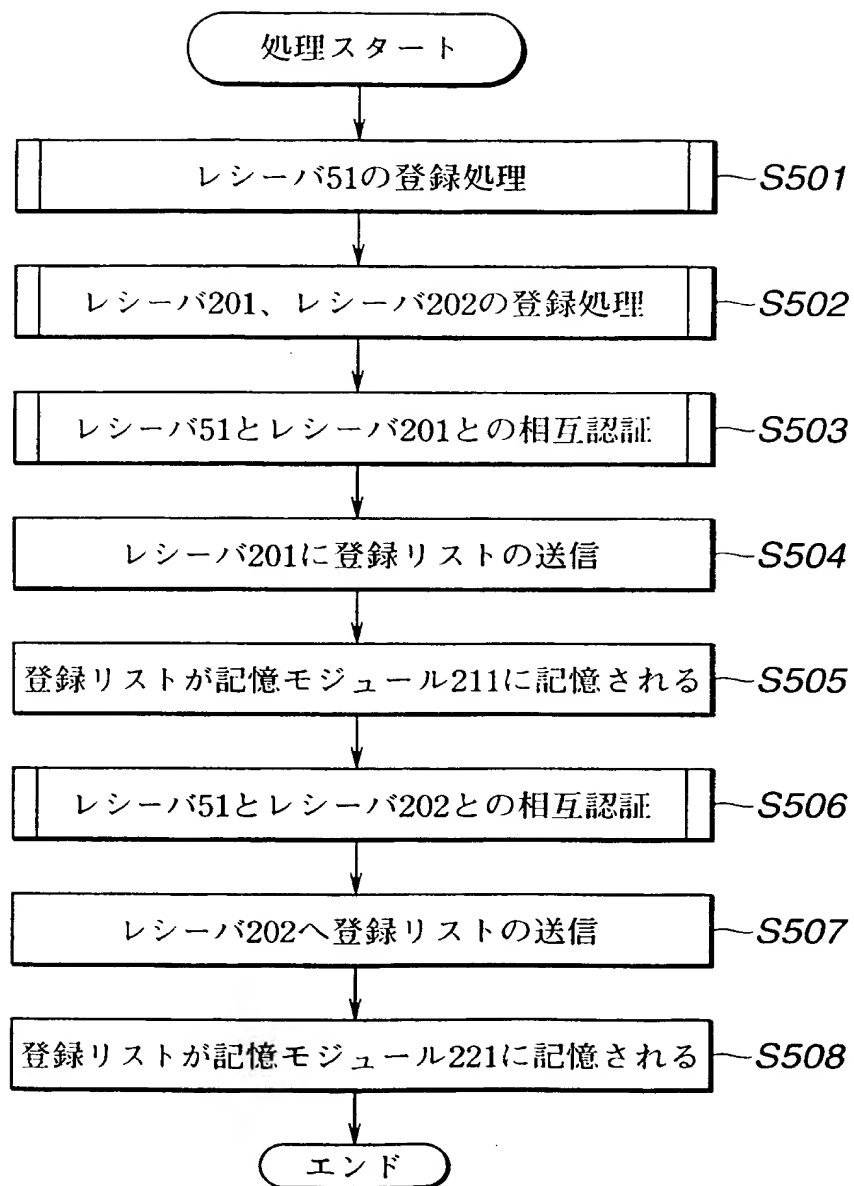


FIG.71

**THIS PAGE BLANK (USPTO)**

---

71/88

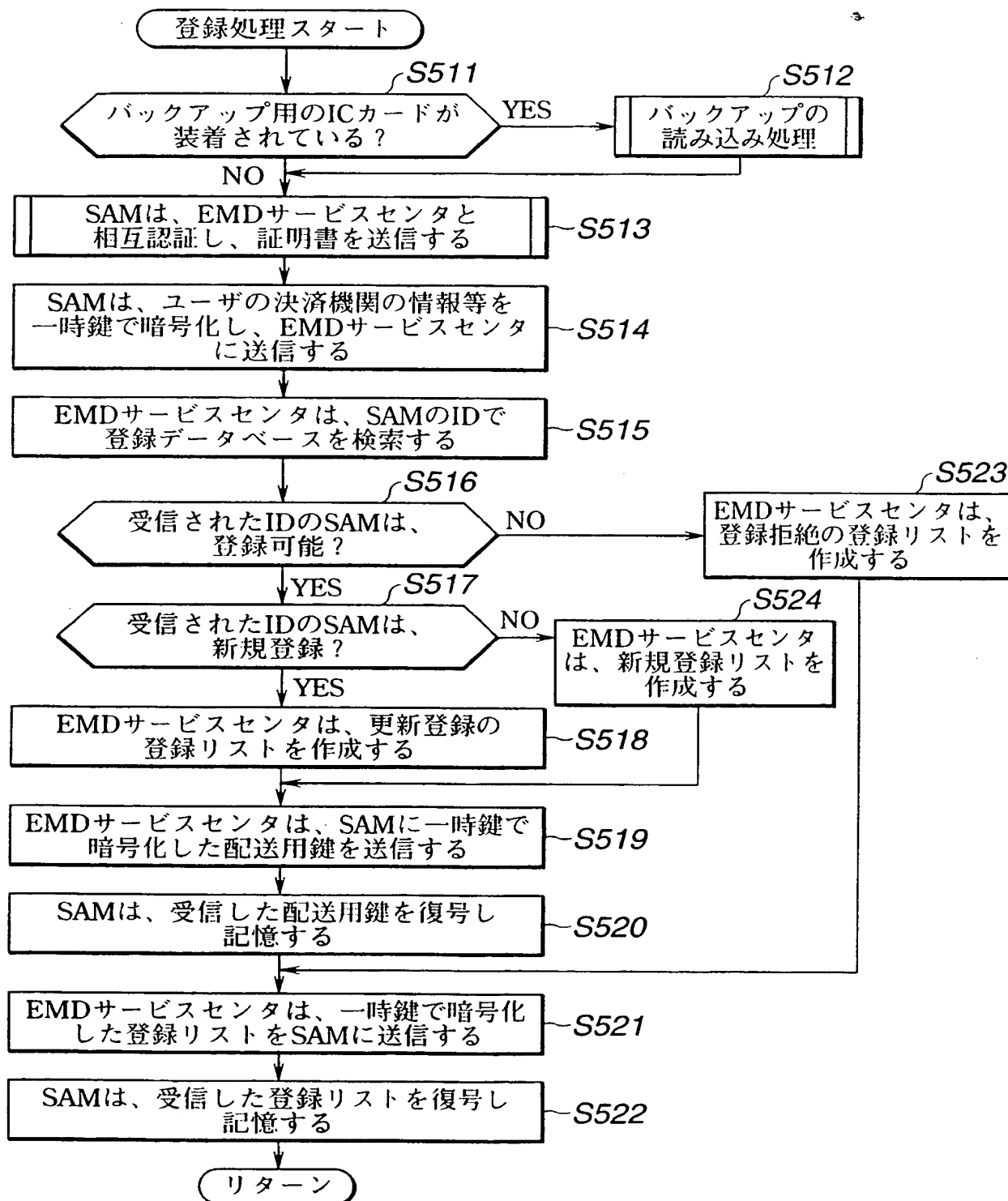


FIG.72

**THIS PAGE BLANK (USPTO)**

レシーバ51の登録条件

SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態情報	登録条件署名	登録リスト署名
SAM62のID	ユーザのID	可	可	SAM62のID	なし	制限なし	XXX	XXXX

登録リスト部

登録リスト

対象SAM ID

SAM62のID

有効期限

XXXXXXXX

バージョン番号

XXXXXXXX

接続されている機器数

3

対象SAM情報部

FIG.73

**THIS PAGE BLANK (USPTO)**



73/88

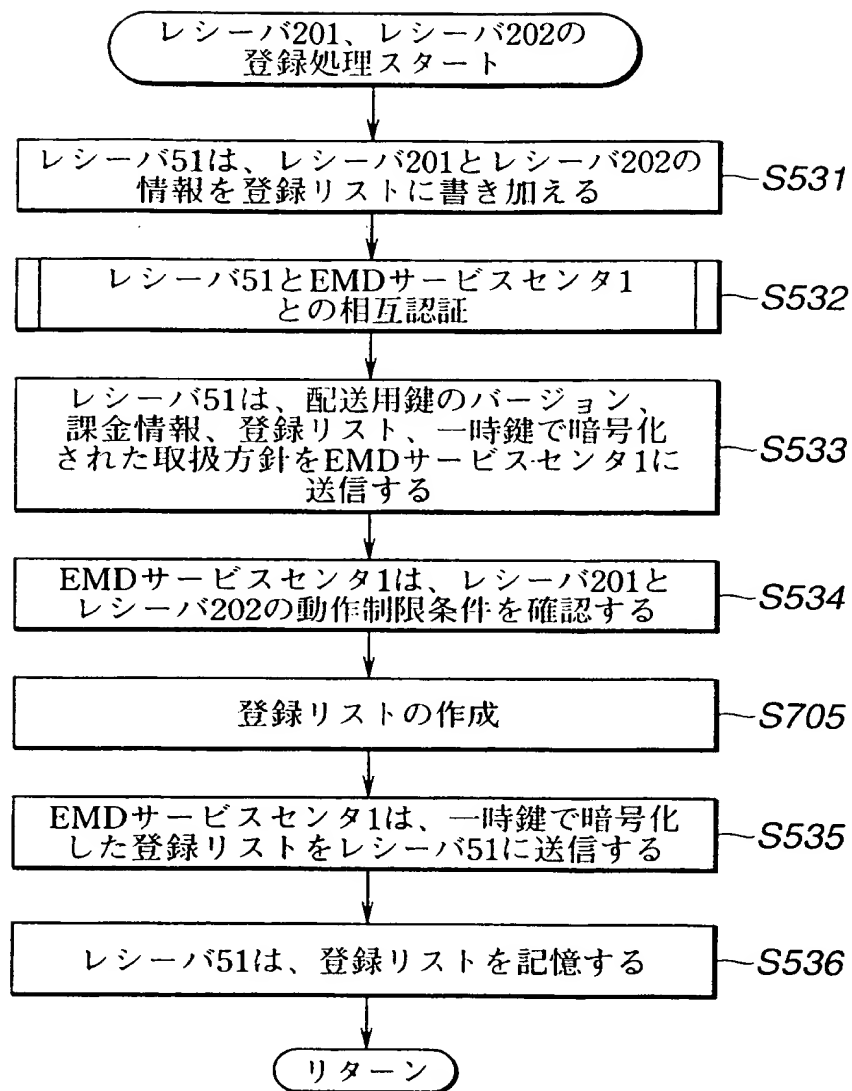


FIG.74

**THIS PAGE BLANK (USPTO)**

レシーバ51の登録条件

SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態情報	登録条件署名	登録リスト署名
SAM62のID	ユーザのID	可	可	SAM62のID	なし	制限なし	×××	××××
SAM210のID		可	不可	SAM62のID	なし	制限なし	×××	
SAM220のID		不可	不可	なし	SAM62のID SAM210のID	制限なし	×××	

リスト部

対象SAM ID

有効期限

バージョン番号

接続されている機器数

SAM62のID	×	×	×	×
	×	×	×	×
				3

対象SAM情報部

FIG.75

**THIS PAGE BLANK (USPTO)**

---

75/88

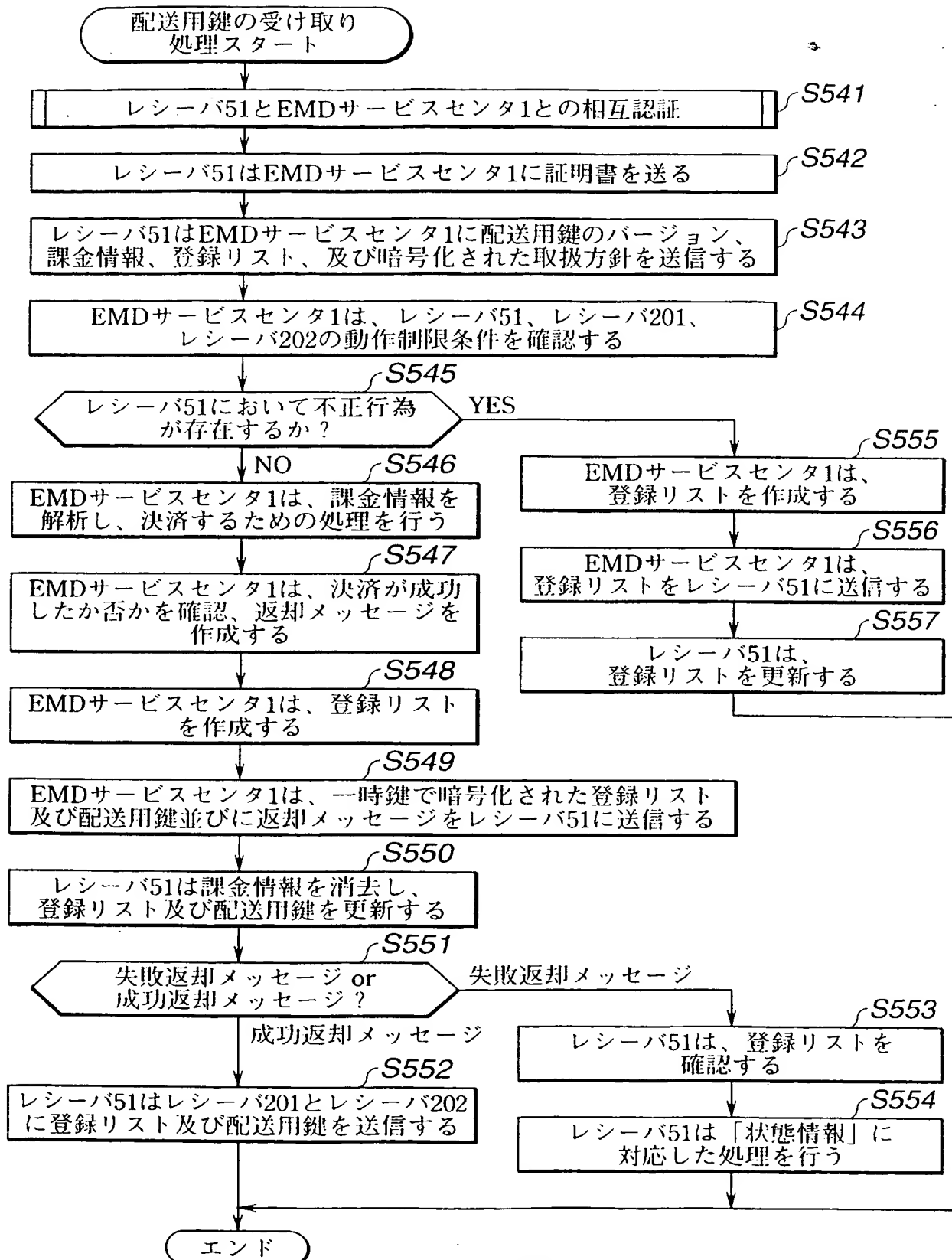


FIG.76

**THIS PAGE BLANK (USPTO)**

76/88

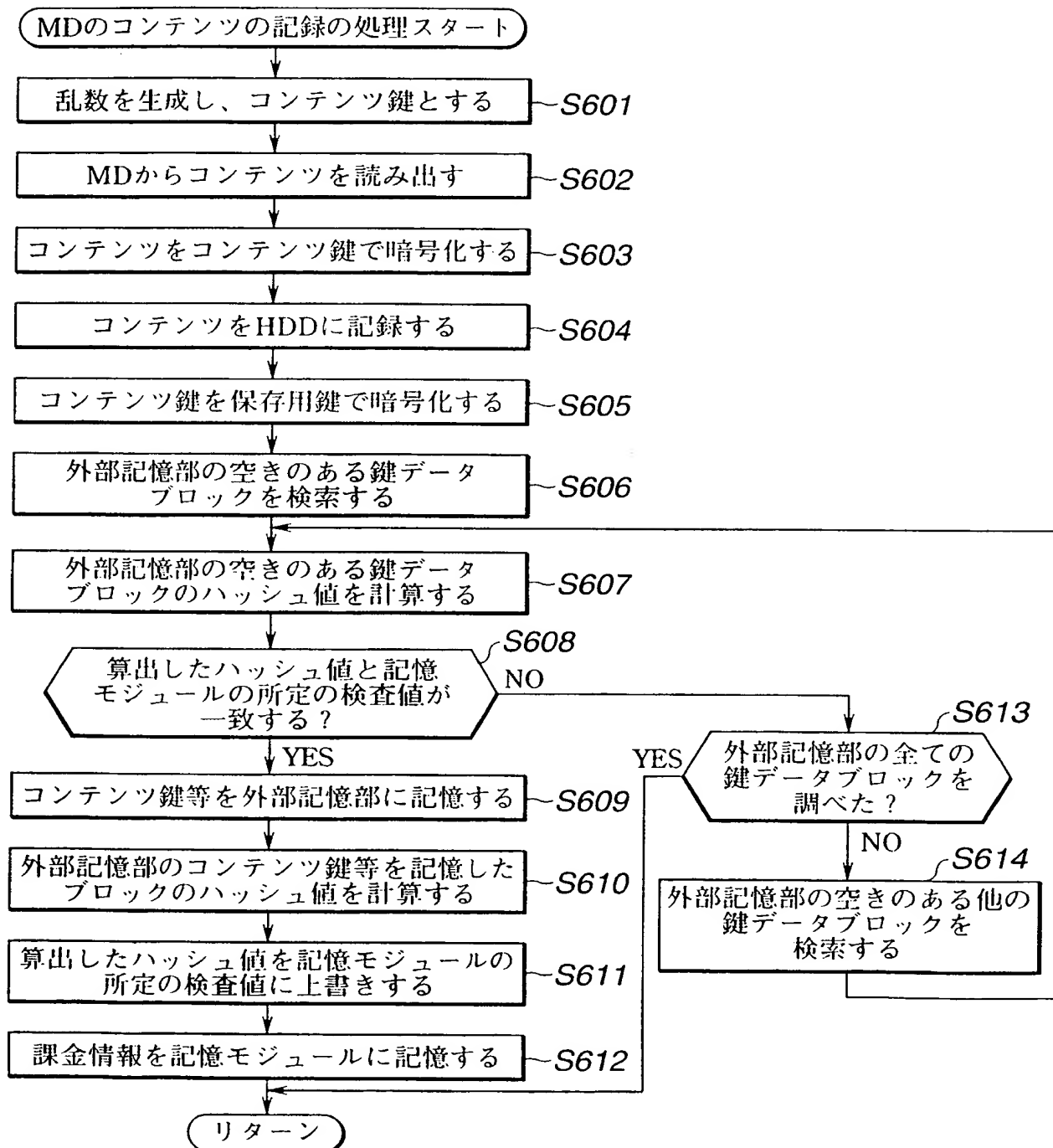


FIG.77

**THIS PAGE BLANK (USPTO)**



77/88

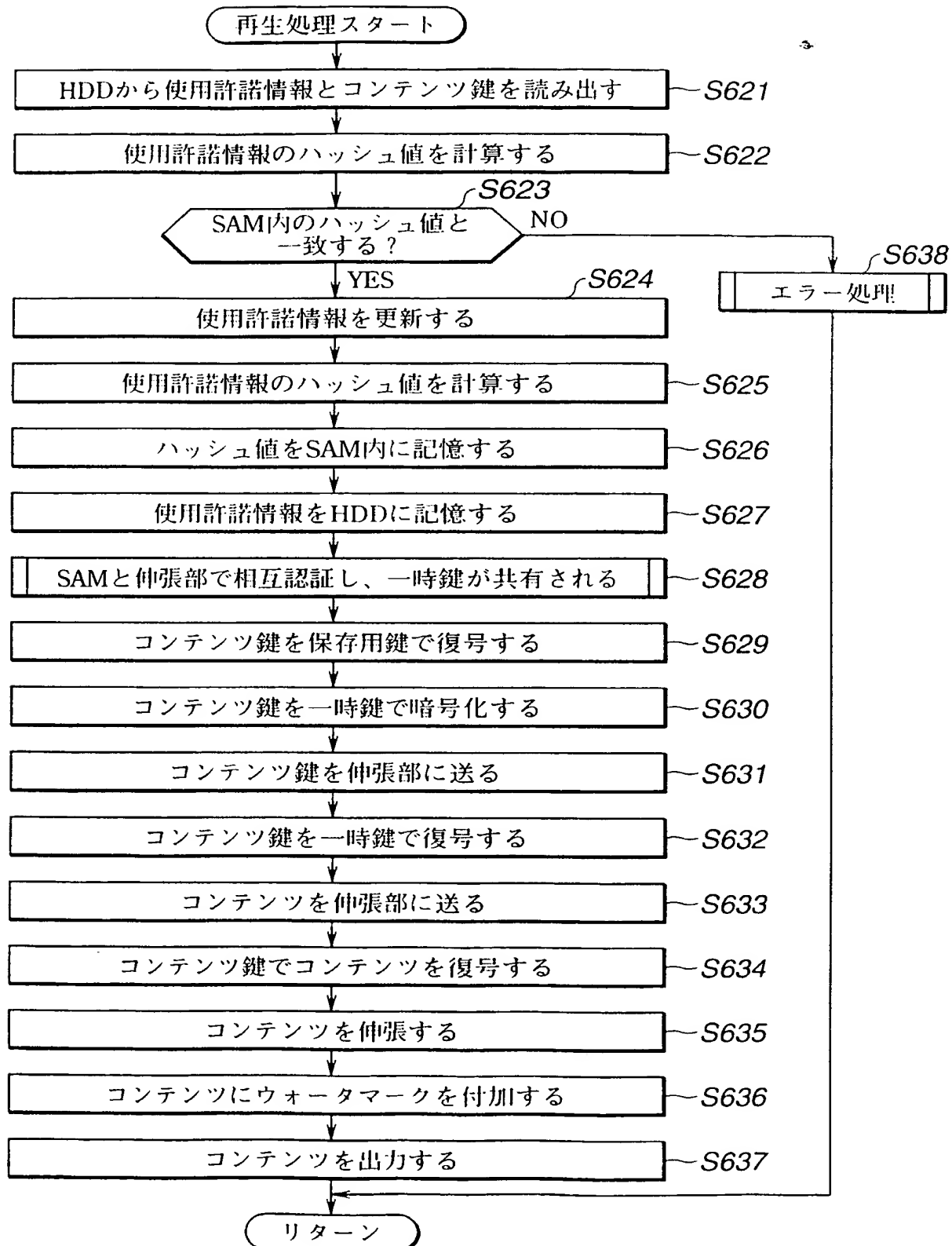


FIG.78

**THIS PAGE BLANK (USPTO)**

78/88

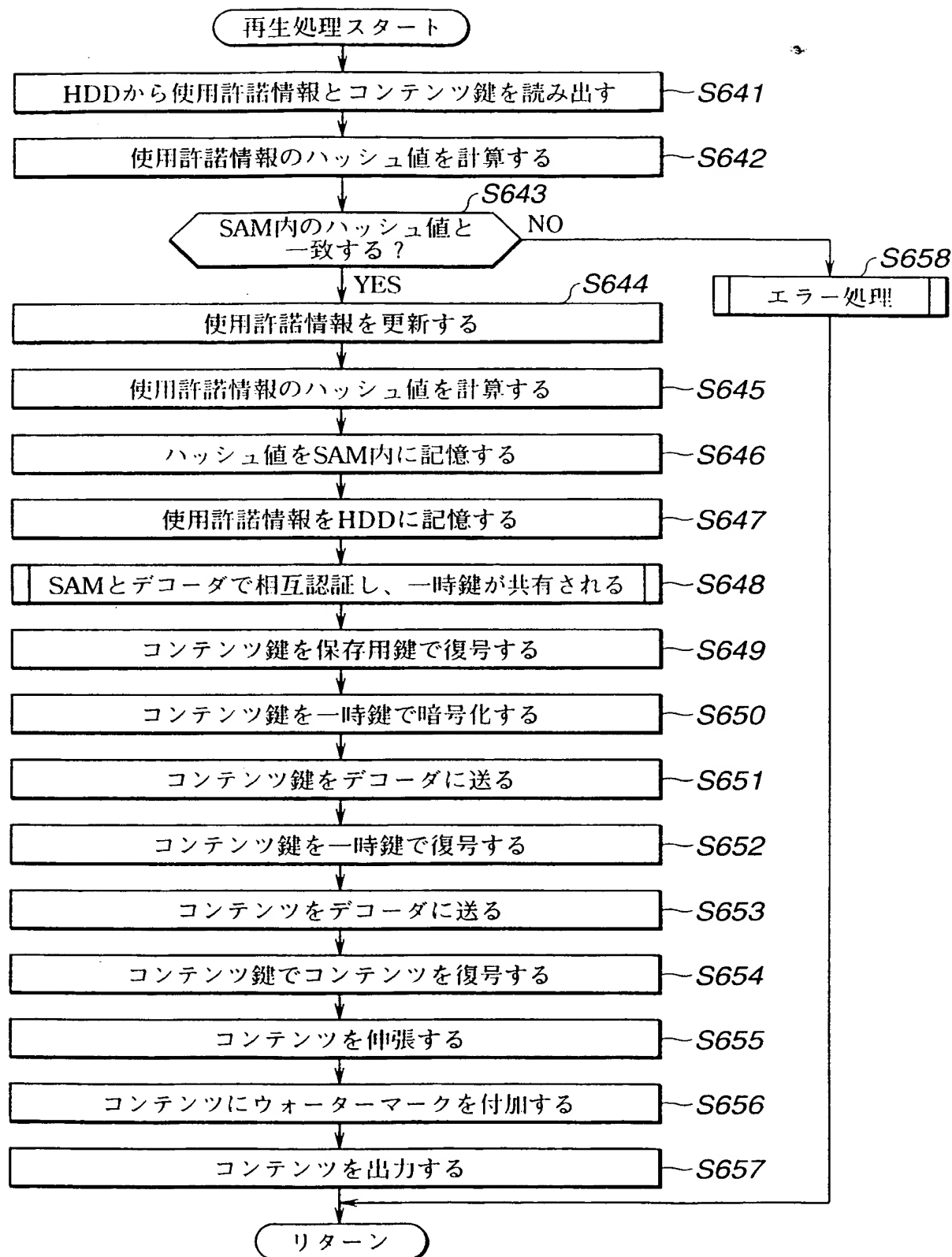


FIG.79

**THIS PAGE BLANK (USPTO)**

---

79/88

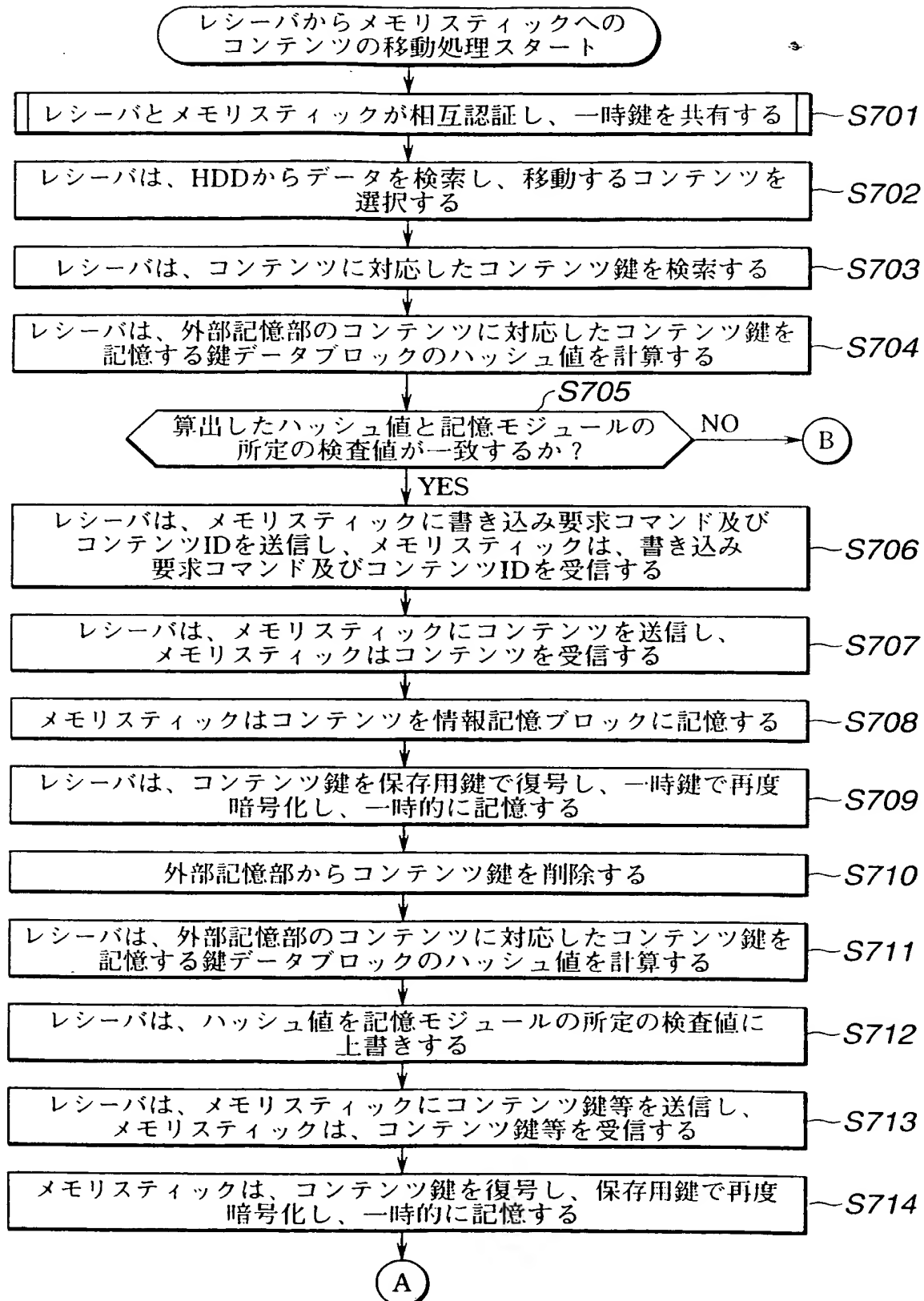


FIG.80

**THIS PAGE BLANK (USPTO)**

---

80/88

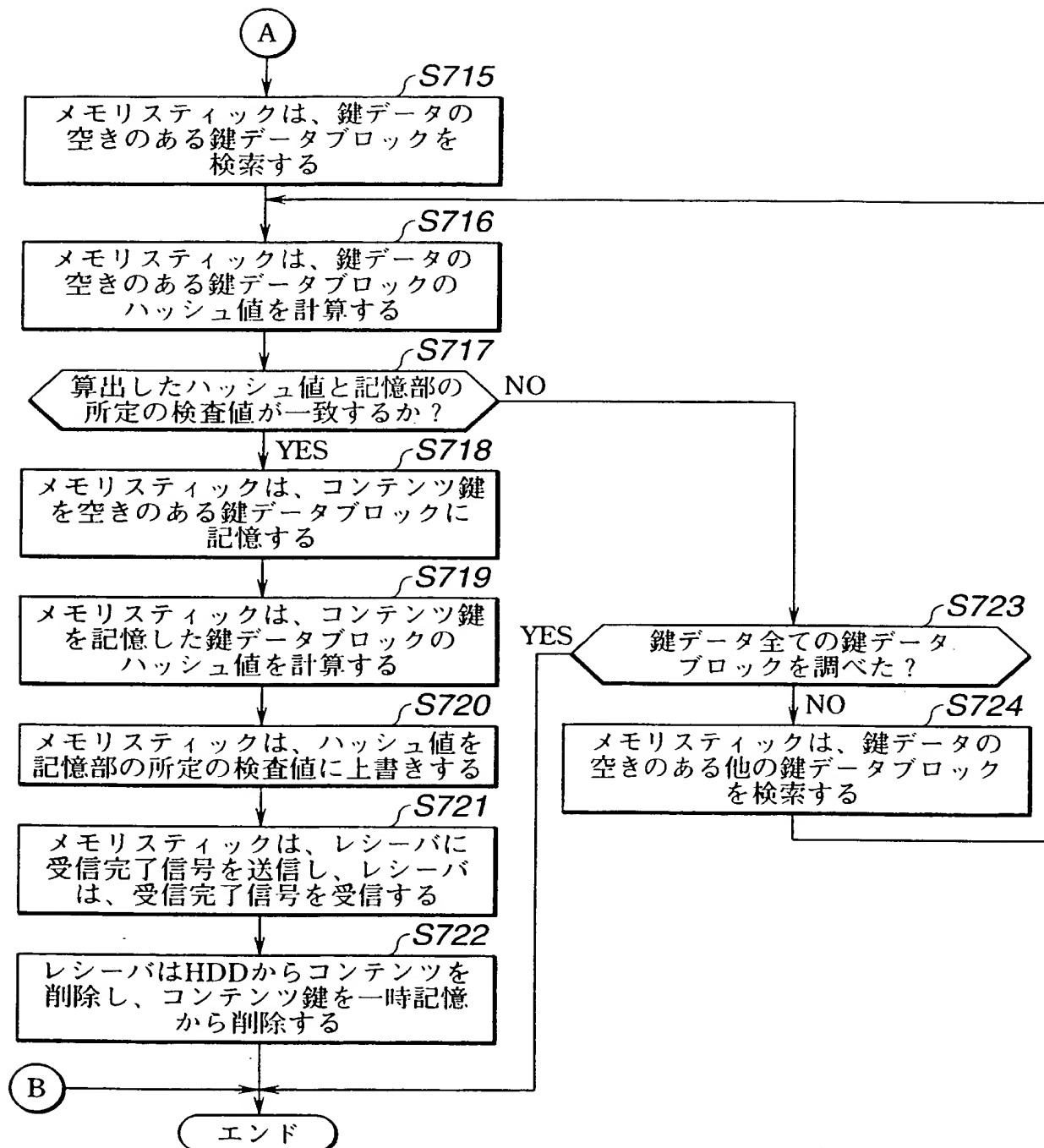


FIG.81

**THIS PAGE BLANK (USPTO)**

---



81/88

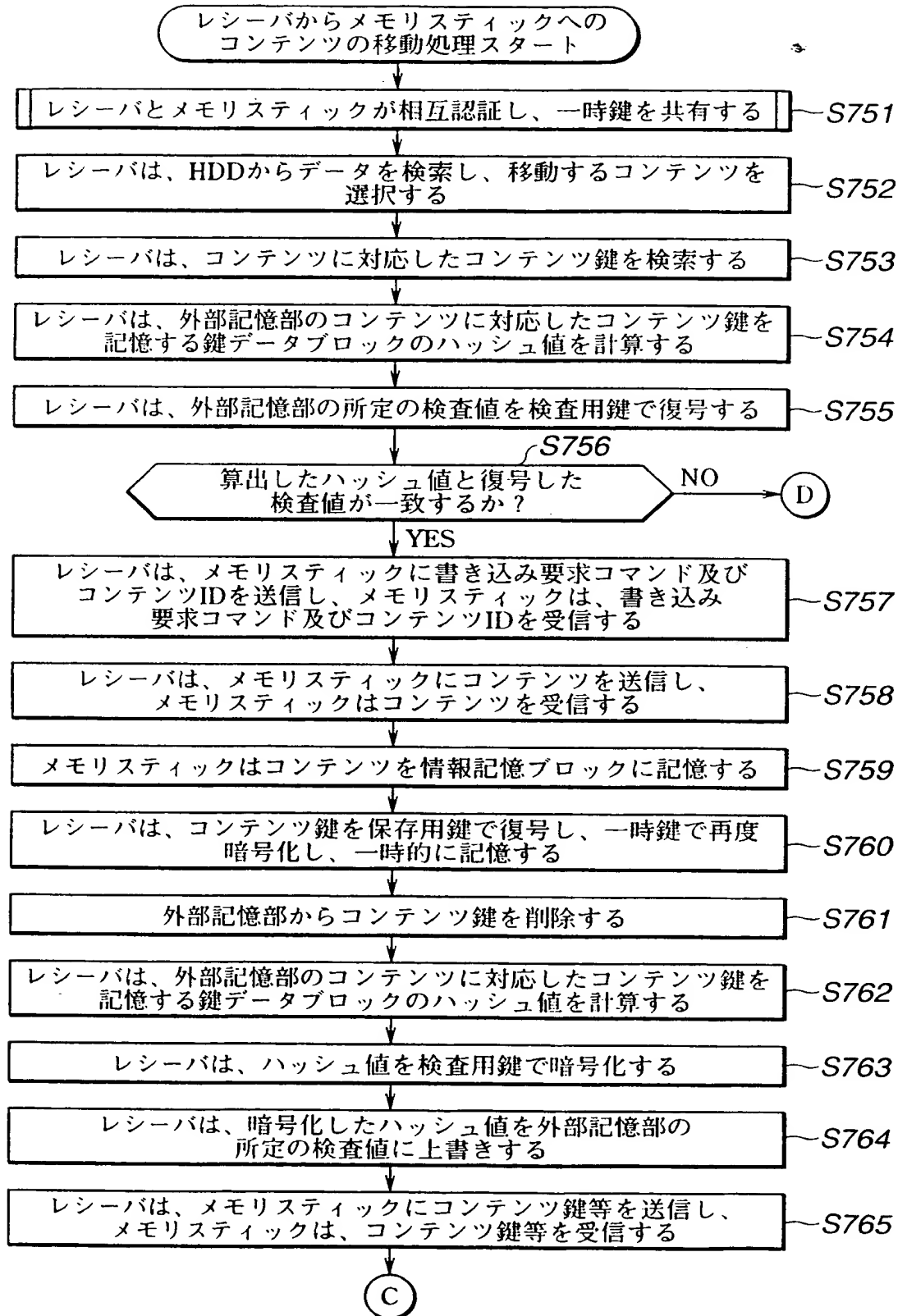


FIG.82

**THIS PAGE BLANK (USPTO)**

---

82/88

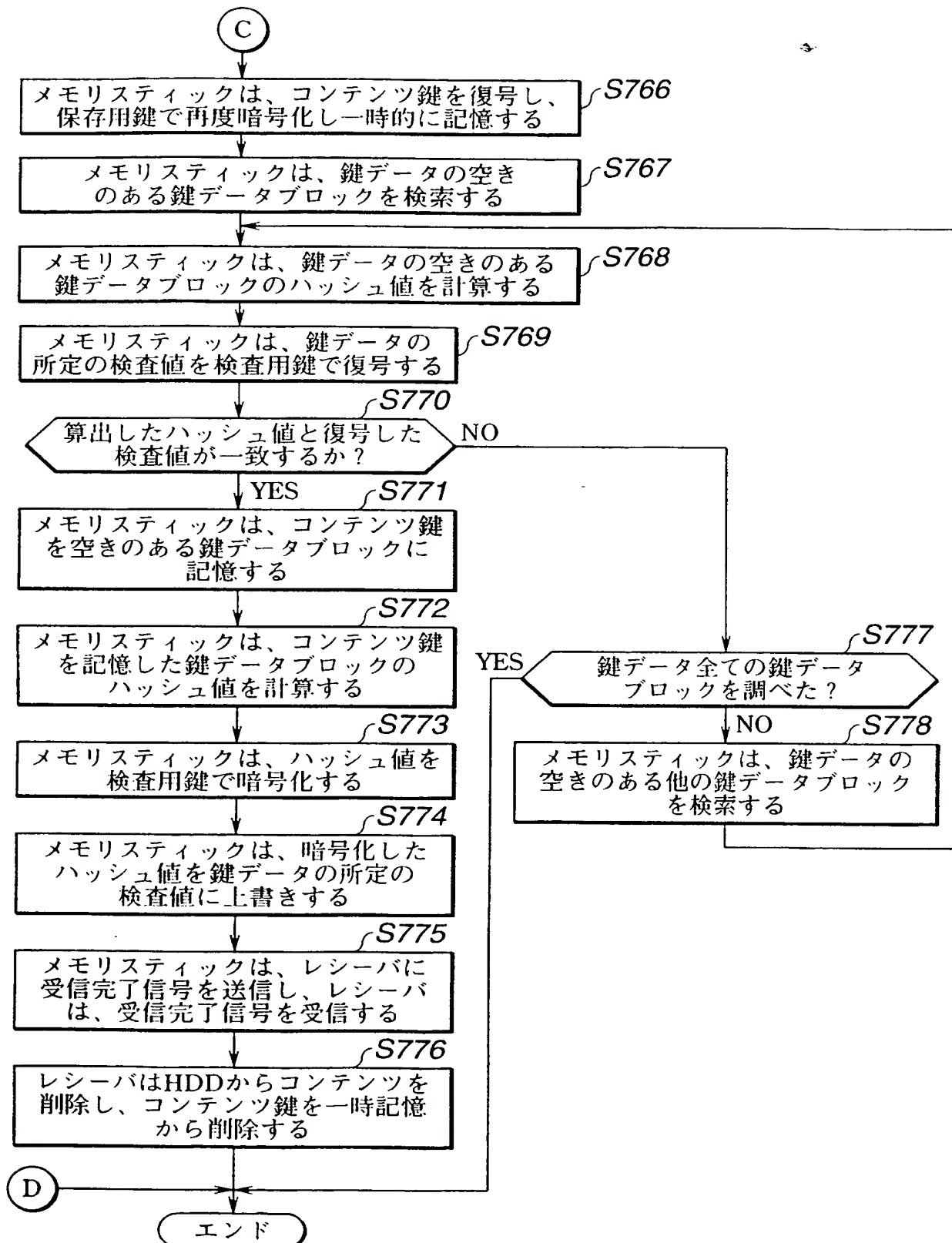


FIG.83

**THIS PAGE BLANK (USPTO)**

---

83/88

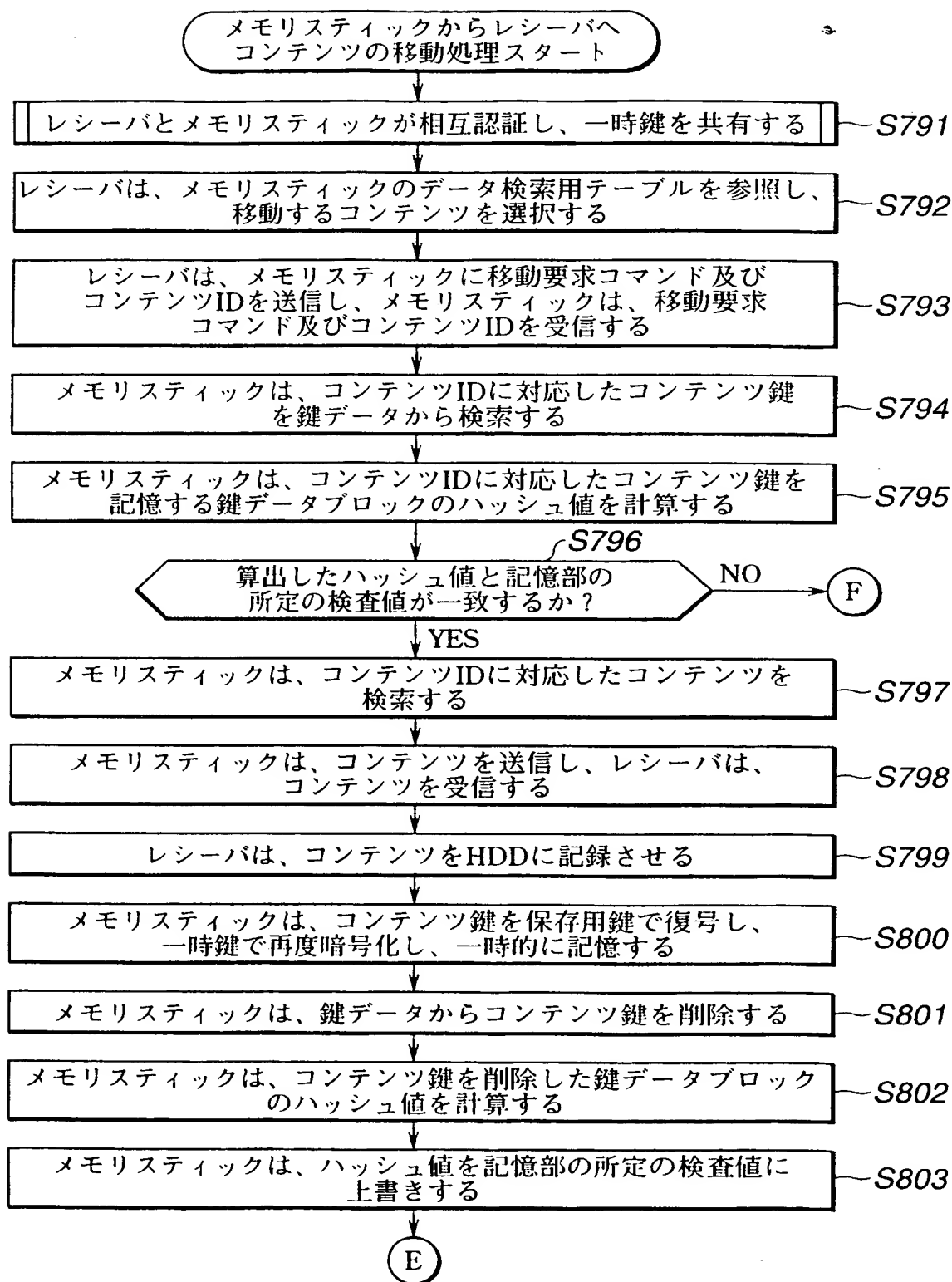


FIG.84

**THIS PAGE BLANK (USPTO)**

84/88

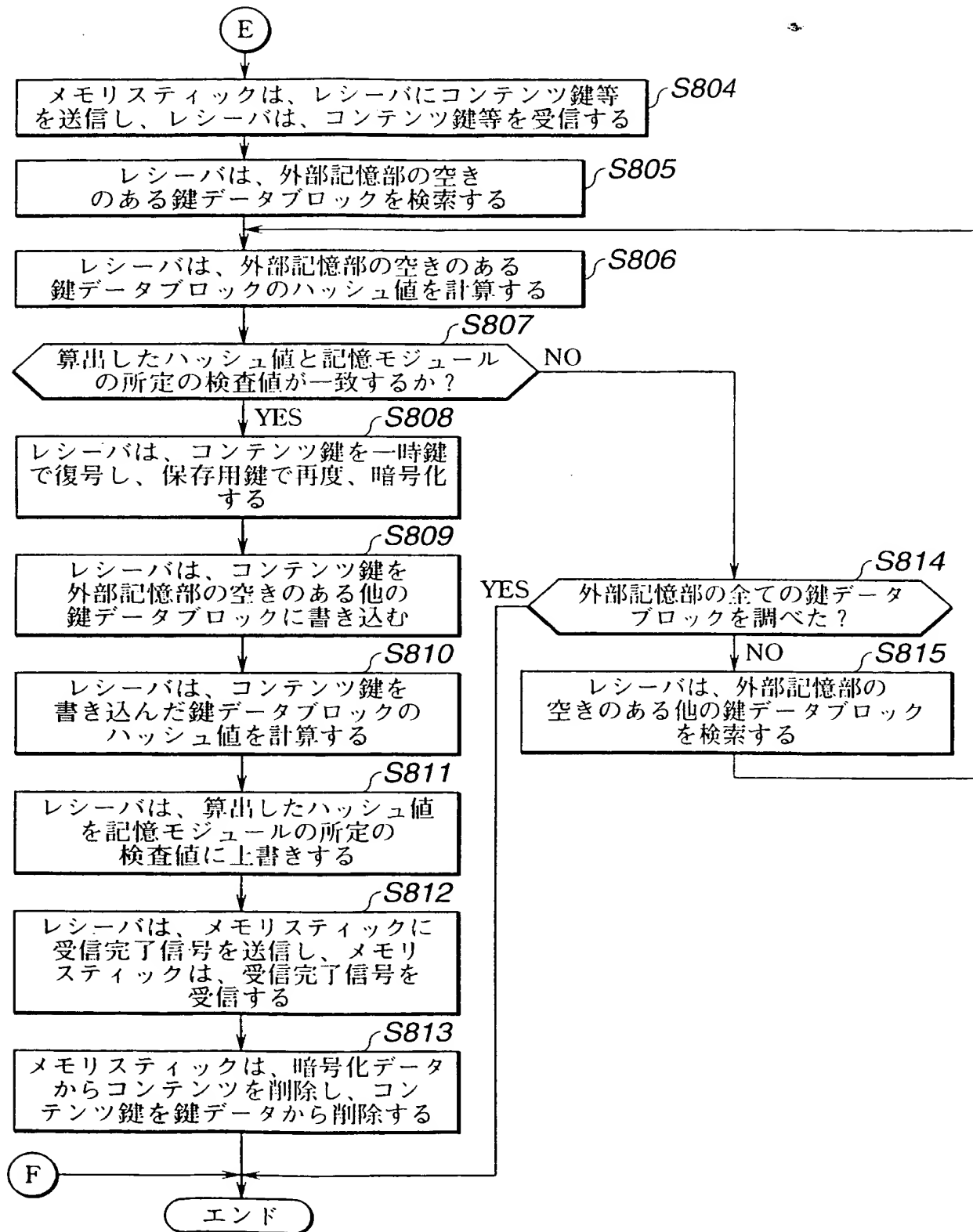


FIG.85

**THIS PAGE BLANK (USPTO)**

---



85/88



FIG.86

**THIS PAGE BLANK (USPTO)**

---

86/88

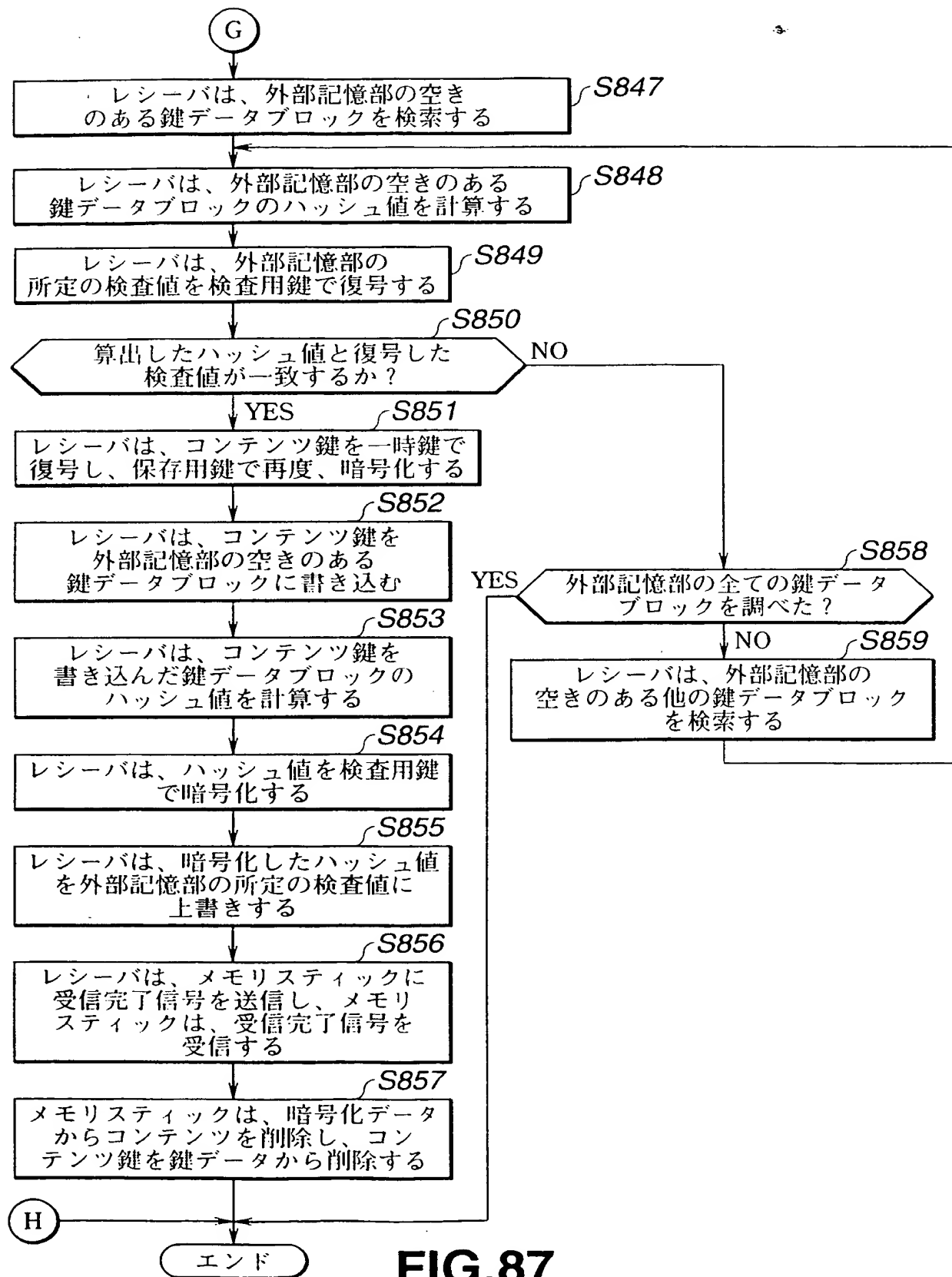


FIG.87

**THIS PAGE BLANK (USPTO)**

---

87/88



FIG.88

**THIS PAGE BLANK (USPTO)**

---

88/88

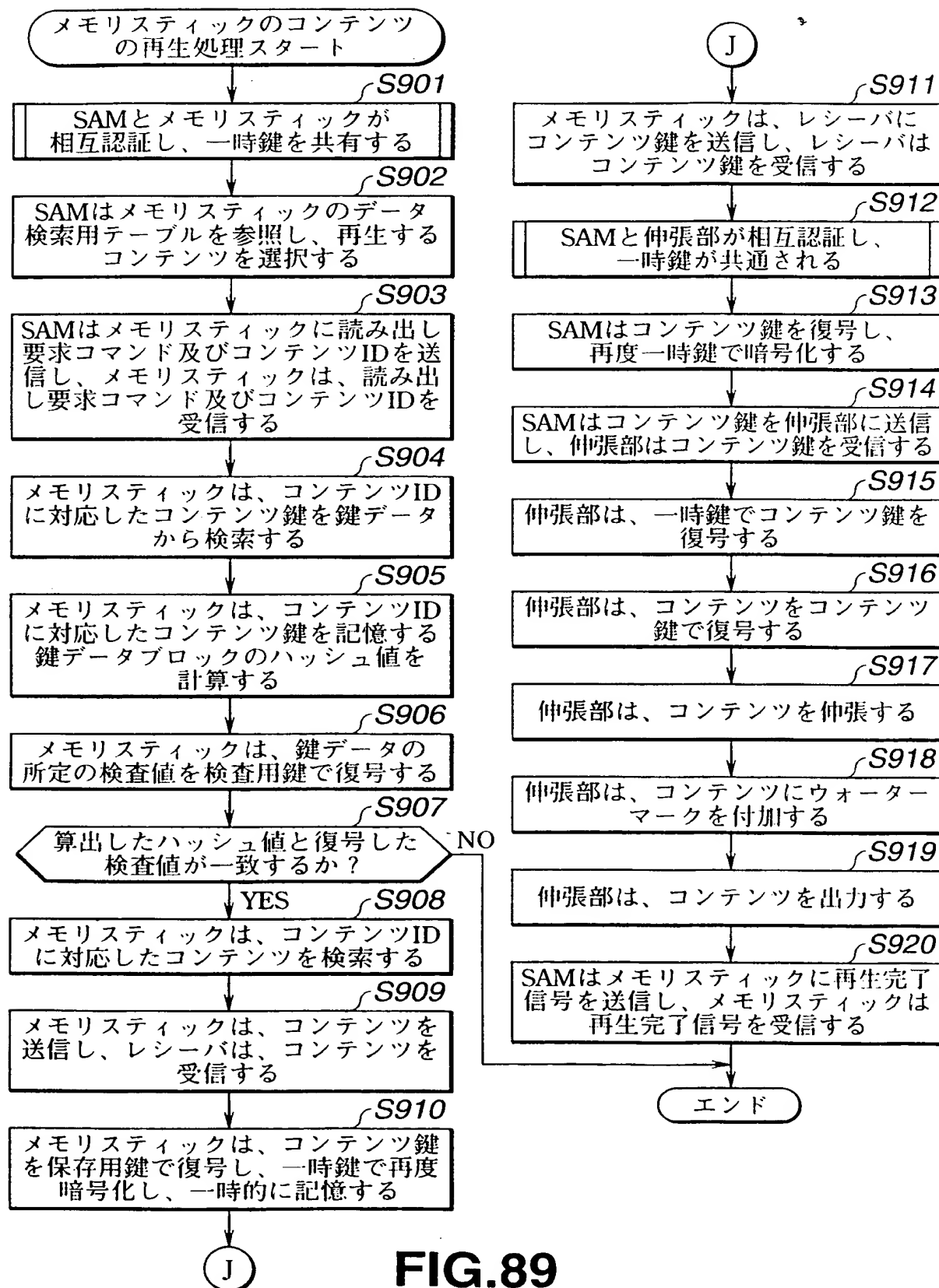


FIG.89

**THIS PAGE BLANK (USPTO)**

---



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/05689

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> G06F15/00, G06F17/60, H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> G06F15/00, G06F17/60, H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000  
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
CS, WPI, JICST contents, distribution, SuperDistribution

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO, 96/27155, A3 (Electronic Publishing Resources, Inc.), 06 September, 1996 (06.09.96), pages 393-394, 607, 630, 785; Fig. 19; pages 393-394, 607, 630, 785, 790 to 791; Fig. 19; pages 169, 487-488, 638-644, 652, 830-832; Fig. 2; pages 487-490; page 480; Fig. 33	1-3 7-9 13-22 33-38 39-42
Y	pages 617-618; Figs 66, 67; pages 633-634; pages 165-166; Fig. 2; pages 485-490; Fig.35	10-12 43-51 52-58 59-66
A	& JP, 10-512074, W & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A & US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	4-6, 23-32, 67

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p>
--	---

Date of the actual completion of the international search  
14 March, 2000 (14.03.00)

Date of mailing of the international search report  
21 March, 2000 (21.03.00)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

International application No.

PCT/JP99/05689

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US, 5701343, A (Nippon Telegraph & Telephone Corp.),	67
Y	23 December, 1997 (23.12.97), Column 8, lines 1 to 34 & JP, 8-160855, A & JP, 8-160856, A & EP, 715242, A1	43-51
Y	EP, 809379, A2 (Matsushita Electric Ind. Co. Ltd.), 26 November, 1997 (26.11.97), Full text & JP, 10-51439, A & TW, 333630, A & KR, 97076418, A	10-12  52-66
Y	US, 5103392, A (Fujitsu Limited), 07 April, 1992 (07.04.92), Full text & JP, 6-95302, B & JP, 6-28030, B & JP, 3-14442, B	
Y	"Protection of the Copyright of Music; "Hadaka" no CD ga genkaini", Nikkei Electronics, Nikkei BP K.K., 15 June, 1998 (15.06.98), No. 718, pages 57-64, Figs. 5,6	54
Y	JP, 9-265254, A (Dainippon Printing Co., Ltd.), 07 October, 1997 (07.10.97), Full text (Family: none)	59-62,66
Y	JP, 7-212742, A (Matsushita Electric Ind. Co., Ltd.), 11 August, 1995 (11.08.95), column 3, lines 22-30 (Family: none)	23,26,27
Y	JP, 7-154770, A (NEC Corporation), 16 June, 1995 (16.06.95), Full text (Family: none)	23,26,27 1-9
A	EP, 840194, A2 (Matsushita Electric Ind. Co. Ltd.), 06 May, 1998 (06.05.98), Full text & JP, 10-133955, A & AU, 695948, B & KR, 98033266, A	1-9

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/05689

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The invention of the present application is categorized in the 12 groups of inventions, namely claims 1-3, 4-6, 7-9, 10-12, 13-22, 23-32, 33-35, 36-38, 39-42, 43-51, 52-58, 59-67.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☐ No protest accompanied the payment of additional search fees.

**THIS PAGE BLANK (USPTO)**

## 国際調査報告

国際出願番号 PCT/J P 99/05689

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F15/00, G06F17/60, H04L9/08

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F15/00, G06F17/60, H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926-1996年
日本国公開実用新案公報	1971-2000年
日本国実用新案登録公報	1996-2000年
日本国登録実用新案公報	1994-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

CSデータベース, WPI, JICST 科学技術文献データベース contents, distribution, SuperDistribution

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	W0, 96/27155, A3 (Electronic Publishing Resources, Inc.) 6.9月.1996(06.09.96), 第393- 394, 607, 630, 785頁, 図19, 第393- 394, 607, 630, 785, 790- 791頁, 図19, 第169, 487- 488, 638- 644, 652, 830- 832頁, 図2, 第487- 490頁, 第480頁, 図33,	1-3 7-9 13-22 33-38 39-42
Y	第617- 618頁, 図66, 67, 第633- 634頁, 第165- 166頁, 図2, 第485- 490頁, 図35	10-12 43-51 52-58 59-66

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

14.03.00

国際調査報告の発送日

21.03.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5M

9364

電話番号 03-3581-1101 内線 3599

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	& JP, 10-512074, W & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A & US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	4-6, 23-32, 67
X	US, 5701343, A (Nippon Telegraph & Telephone Corp.)	67
Y	23.12月.1997(23.12.97), 第8欄第1-34行 & JP, 8-160855, A & JP, 8-160856, A & EP, 715242, A1	43-51
Y	EP, 809379, A2 (Matsushita Electric Ind. Co. Ltd.) 26.11月.1997(26.11.97), 全頁を参照 & JP, 10-51439, A & TW, 333630, A & KR, 97076418, A	10-12
Y	US, 5103392, A (Fujitsu Limited) 7.4月.1992(07.04.92), 全頁を参照 & JP, 6-95302, B & JP, 6-28030, B & JP, 3-14442, B	52-66
Y	音楽の著作権保護, 「裸」のCDが限界に, 日経エレクトロニクス, 日経BP社, 15.6月.1998(15.06.98) no.718, p.57-64, 図5,6	54
Y	JP, 9-265254, A (大日本印刷株式会社) 7.10月.1997(07.10.97), 全頁を参照 (ファミリーなし)	59-62, 66
Y	JP, 7-212742, A (松下電器産業株式会社) 11.8月.1995(11.08.95), 第3欄第22-30行 (ファミリーなし)	23, 26, 27
Y A	JP, 7-154770, A (日本電気株式会社) 16.6月.1995(16.06.95), 全頁を参照 (ファミリーなし)	23, 26, 27 1-9
A	EP, 840194, A2 (Matsushita Electric Ind. Co. Ltd.) 6.5月.1998(06.05.98), 全頁を参照 & JP, 10-133955, A & AU, 695948, B & KR, 98033266, A	1-9

## 第Ⅰ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査することを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

この出願の発明は、請求の範囲 1-3, 4-6, 7-9, 10-12, 13-22, 23-32, 33-35, 36-38, 39-42, 43-51, 52-58, 59-67 の 12 群の発明に区分される。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

**THIS PAGE BLANK (USPTO)**